Version 5.0

Benutzerhandbuch

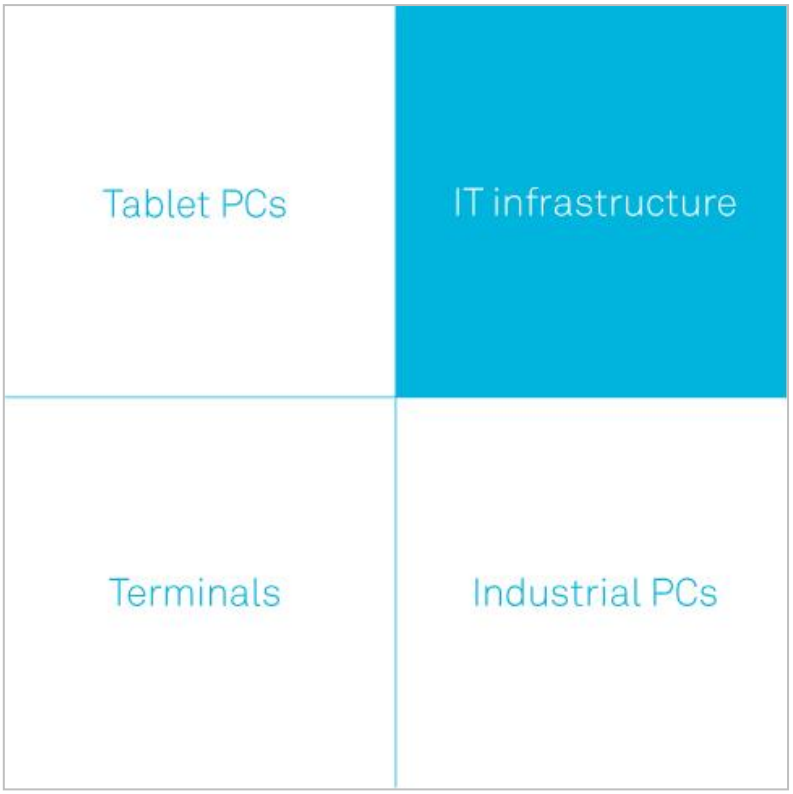
IT Infrastructure

RAP/RAC1000

adstec

the rugged world of IT®

Product Portfolio



Copyright
© ads-tec GmbH
Heinrich-Hertz-Str. 1
72622 Nürtingen
Germany

ANWENDUNGEN MIT HOHEM RISIKO

Der Access Point/Client verfügt, sofern nicht ausdrücklich in der Produktdokumentation anders beschrieben, über keine Fehlertoleranz und ist nicht für die Verwendung oder den Wiederverkauf als Online-Kontrollausrüstung in Umgebungen, die fehlerfreie Leistungen erfordern, konzipiert, hergestellt oder ausgerichtet, wie zum Beispiel die Verwendung in Kernkraftanlagen, Flugzeugnavigations- oder Kommunikationssystemen, bei der Luftverkehrskontrolle, in Lebensrettungs- oder Waffensystemen, bei denen der Ausfall des Access Points/Clients zu Tod, Personenschäden oder schweren physikalischen oder Umweltschäden führen kann (Anwendungen mit hohem Risiko). ads-tec und seine Zulieferer übernehmen keinerlei ausdrückliche oder stillschweigende Garantie bezüglich der Eignung des Access Points/Clients für Anwendungen mit hohem Risiko.

INHALTSVERZEICHNIS

Wir über uns 6

1 Anmerkungen 7

1.1 Allgemeine Anmerkung 7
1.2 Relevante Dokumentationen zum Gerät 7
1.3 Erklärung zu den verwendeten Symbolen 7
1.4 Daten, Abbildungen, Änderungen 7
1.5 Warenzeichen 8
1.6 Urheberrecht 9
1.7 Normen 9

2 Betriebs-/ Sicherheitshinweise 10

2.1 Sicherheitshinweise 10
2.2 Betriebsort 11
2.3 Schäden durch unsachgemäßen Gebrauch 11
2.4 Gewährleistung / Reparatur 11
2.5 Allgemeine Hinweise zur 5GHz Version (802.11 A / 802.11 H) ETSI 12
2.6 Antennenübersicht für den Einsatz in USA und Canada / FCC 13
2.7 Kanalübersicht für den Einsatz in USA und Canada / FCC 14
2.8 WLAN Hinweise 14

3 Einleitung 15

3.1 Ausstattungsvarianten 16
3.2 Lieferumfang 17
3.3 Umweltbedingungen 17

4 Montage 18

4.1 Montagemöglichkeit 18
4.2 Außenabmessungen des Geräts 18
4.3 Montageskizze des Gerätes 20
4.4 Befestigung des Geräts 21
4.5 Anschluss der Versorgungsleitungen 22
4.6 Montage der Antennen 24

5 Systemmerkmale 25

5.1 Allgemeine LED Status-Anzeigen 25
5.2 Betriebsbedingte LED Status-Anzeigen 26
5.3 Schnittstellenübersicht 29

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

6 Inbetriebnahme 32

6.1 Erst-Konfiguration 32
6.2 Manuelle Konfiguration des Netzwerkadapters über das RJ45/LWL-Kabel 32
6.3 Konfiguration des WLAN-Netzwerkadapters 34
6.4 Erstkonfiguration im Geräte-Webinterface 36
6.5 Konfiguration des WLAN- Netzes 37
6.6 Herstellen einer Verbindung mit dem Drahtlos-Netzwerk 37

7 Access Point Setup-Assistent 38

7.1 Erstkonfiguration mit Hilfe des Setup-Assistenten 38
7.1.1 IP-Konfiguration 39
7.1.2 WLAN-1 Konfiguration 41
7.1.3 Passwort ändern 47
7.2 Konfiguration mit Hilfe des Paketfilteres 49
7.2.1 Hinzufügen einer Regel 49
7.2.2 Ändern und Suchen von bestehenden Regelsets 50
7.2.3 Laden einer vorkonfigurierten Regel 51
7.2.4 Neues Regelset auf Layer 2 definieren 53
7.2.5 Neues Regelset auf Layer 3 definieren 63

8 Access Point/Client Weboberfläche 76

8.1 Hauptmenüpunkt Diagnose 76
8.1.1 Systemstatus 76
8.2 Allgemeine Übersicht zur Konfiguration in den Menüs 77
8.2.1 Beispielkonfiguration IP-Routing 78
8.2.2 Fehlermeldungen 80
8.2.3 Eventlog 81
8.2.4 ICS-Status 82
8.2.5 HOST 82
8.2.6 Ping Test 83
8.2.7 Remote Capture 84
8.3 Hauptmenüpunkt Konfiguration 84
8.3.1 IP-Konfiguration 84
8.3.2 WLAN-1 Parameter 91
8.3.3 WLAN-1 Sicherheit 99
8.3.4 Statische MAC-Adresse 103
8.3.5 Paketfilter 105
8.3.6 Grundeinstellungen 106
8.3.7 Zugriffsrechte 111
8.3.8 Adv.WLAN 115
8.3.9 Sonstiges 119
8.3.10 Netzwerk 120
8.3.11 Dienste 127
8.3.12 Priorisierung 133
8.4 Hauptmenüpunkt System 135
8.4.1 Backup Einstellungen 135
8.4.2 Softwareupdate 137
8.4.3 Werkseinstellungen 139
8.4.4 Speichern 140
8.4.5 Neustart 140
8.6 Hauptmenüpunkt Informationen 141
8.6.1 Allgemein 141
8.6.2 Technische Daten 142
8.6.3 Geräteinstallation 143
8.6.4 Lokale Diagnose 143

8.6.5 Inhaltsverzeichnis 144

9 Zulassungen 145

9.1 Europazulassungen 145
9.1 Kanallisten 147
9.2 5 GHz DFS Reglementierung nach ETSI EN 301 893 V1.4.1 innerhalb der EU 155
9.3 FCC-Approval 156
9.4 Richtlinien 157

10 Technische Details 158

10.1 Varianten 158
10.2 Datenübertragung Ethernet 158
10.3 Funk Eigenschaften 159
10.4 Energieversorgung 159
10.5 Konfiguration 159
10.6 Allgemeine Daten 159

11 Service und Support 160

11.1 ads-tec Support 160
11.2 Firmenadresse 160

12 Anwendungsbeispiele 161

12.1 Priorisierung 161
12.2 Zertifikate 166
12.3 SIM-Karte 191
12.4 USB-Drucker 193
12.5 Übersicht der Client Betriebsmodi 195
12.6 Extended Backround Scanning und Router 197
12.7 Seamless Roaming 202
12.8 Extended Backround Scanning 207
12.9 Erweiterte Roaming Parameter 211
12.1 Remote Capture 216

13 CE-Konformitätserklärung 220

13.1 Zulassung Brasilien 236

WIR ÜBER UNS

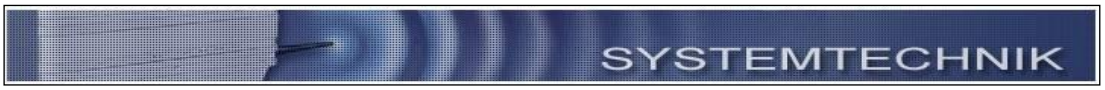
©ads-tec GmbH
Heinrich-Hertz-Str. 1
72622 Nürtingen
Germany

Tel: +49 7022 2522-0
Fax: +49 7022 2522-400
E-Mail: mailbox@ads-tec.de
Home: www.ads-tec.de

Als Technologielieferant unterstützt ads-tec große Unternehmen und weltweit operierende Konzerne mit modernster Technik, stets aktuellem Know-how und umfangreichen Serviceleistungen im Bereich der Automatisierungs-, Daten- und Systemtechnik.

ads-tec realisiert komplette Automationslösungen von der Planung bis zur Inbetriebnahme und hat sich insbesondere auf die Bereiche Handhabungs- und Greifertechnik spezialisiert.

Der Bereich Datentechnik entwickelt und fertigt PC-basierte Lösungen und verfügt über ein breites Spektrum an Industrie-PCs, Thin-Clients und embedded-Systemen.



ads-tec hat sich auf die Anpassung und Optimierung von Betriebssystemen spezialisiert und entwickelt Softwaretools als Ergänzung zu den angebotenen Hardware-Plattformen.

1 ANMERKUNGEN

1.1 ALLGEMEINE ANMERKUNG

Diese Betriebsanleitung dient dem sicheren und effizienten Umgang mit dem Gerät. Sie muss allen Personen, welche an der Installation und Inbetriebnahme beteiligt sind zugänglich sein und vor Beginn aller Arbeiten gelesen und verstanden werden.
Sie ist nach der Inbetriebnahme dem Geräte-/Anlagenbetreiber zu übergeben.

Alle angegebenen Sicherheitshinweise und Handlungsanweisungen sind Voraussetzung für sicheres Arbeiten und müssen eingehalten werden.

Abbildungen in dieser Anleitung dienen dem grundsätzlichen Verständnis und können von der tatsächlichen Ausführung abweichen.

Das Original dieser Betriebsanleitung wurde in deutscher Sprache verfasst. Jede nicht deutschsprachige Ausgabe dieser Betriebsanleitung ist eine Übersetzung der deutschen Betriebsanleitung.

1.2 RELEVANTE DOKUMENTATIONEN ZUM GERÄT

Für die Einrichtung und den Betrieb des Geräts sind folgende Dokumentationen maßgebend:

BENUTZERHANDBUCH (DIESE DOKUMENTATION):

Enthält Informationen zur Montage, Inbetriebnahme und Bedienung des Geräts sowie die technischen Daten der Gerätehardware.

SERVICE CD:

Enthält Benutzerhandbuch, Montageanleitung, Quick Install Guide und Tools.

1.3 ERKLÄRUNG ZU DEN VERWENDETEN SYMBOLEN

Achtung:
Das Symbol „Achtung“ bezieht sich auf Handlungen, die einen Personenschaden oder einen Schaden der Hard- und Software zur Folge haben können!

Hinweis:
Das Symbol „Hinweis“ vermittelt Bedingungen, die für einen fehlerfreien Betrieb unbedingt beachtet werden müssen. Außerdem werden Tipps und Ratschläge für den effizienten Geräteeinsatz und die Softwareoptimierung gegeben.

1.4 DATEN, ABBILDUNGEN, ÄNDERUNGEN

Texte, Daten und Abbildungen sind unverbindlich. Änderungen, die dem technischen Fortschritt dienen, sind vorbehalten. Unsere Produkte entsprechen den aktuellen gesetzlichen Bestimmungen und Vorschriften zu dem Zeitpunkt, in dem das Produkt unser Haus verlassen hat. Für die Einhaltung und Beachtung darauf folgender technischer oder gesetzlicher Neuerungen wie auch der Betreiberpflichten ist der Betreiber eigenständig verantwortlich.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

1.5 WARENZEICHEN

Es wird darauf hingewiesen, dass die in dieser Dokumentation verwendeten Soft- und Hardwarebezeichnungen sowie Markennamen der jeweiligen Firmen dem allgemeinen warenzeichen-, marken- oder patentrechtlichen Schutz unterliegen.

Windows®, Windows® CE sind eingetragene Warenzeichen der Microsoft Corp.
Intel®, Pentium®, Atom™ , Core™2 , sind eingetragene Warenzeichen der Intel Corp.
IBM®, PS/2® und VGA® sind eingetragene Warenzeichen der IBM Corp.
CompactFlash® ist ein eingetragenes Warenzeichen der Compact Flash Association.
RITTAL® ist ein eingetragenes Warenzeichen der Rittal Werk Rudolf Loh GmbH & Co. KG.

Alle sonstigen national und international bekannten Warenzeichen und Produktnamen werden hiermit anerkannt.

1.6 URHEBERRECHT

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jede Drittverwendung des Handbuchs, die von den urheberrechtlichen Bestimmungen abweicht, ist verboten. Die Reproduktion, die Übersetzung sowie die elektronische und fotografische Archivierung und Veränderung bedarf der schriftlichen Genehmigung der Firma ads-tec GmbH.

Zuwiderhandlung verpflichtet zu Schadenersatz.

1.7 NORMEN

Das Gerät erfüllt die Anforderungen und Schutzziele der folgenden EG-Richtlinien:

- Das Gerät entspricht den Prüfvorschriften für das CE-Zeichen nach den europäischen Prüfnormen EN 61000-6-4 und EN 61000-6-2
- Das Gerät entspricht den Prüfvorschriften DIN EN 60950 (VDE0805, IEC950) „Sicherheit von Einrichtungen der Informationstechnik“
- Das Gerät entspricht den Prüfvorschriften DIN EN 60068-2-6 (Sinusanregung)
- Das Gerät entspricht den Prüfvorschriften DIN EN 60068-2-27 (Schocktest)

Hinweis:

Eine entsprechende Konformitätserklärung wird für die zuständige Behörde beim Hersteller bereitgehalten und kann auf Anfrage eingesehen werden.

Zur Einhaltung der gesetzlichen EMV-Anforderung müssen die angeschlossenen Komponenten sowie die Kabelverbindungen ebenfalls diesen Anforderungen genügen. Es müssen daher abgeschirmte Bus- und LAN-Kabel mit geschirmten Steckern benutzt und diese gemäß den Hinweisen im Benutzerhandbuch installiert werden.

2 BETRIEBS-/ SICHERHEITSHINWEISE

Das Gerät enthält elektrische Spannungen und hochempfindliche Bauteile. Eingriffe des Anwenders sind nur zum Verbinden der Anschlussleitungen vorgesehen. Sollen weitergehende Änderungen vorgenommen werden, so ist der Hersteller oder ein von diesem autorisierter Service zu Rate zu ziehen. Das Gerät muss bei Arbeiten spannungsfrei sein. Es sind geeignete Maßnahmen zur Vermeidung von elektrostatischen Entladungen auf Bauteile zu treffen. Wenn das Gerät von einer nicht autorisierten Person geöffnet wird, können Gefahren für den Benutzer entstehen und der Gewährleistungsanspruch erlischt.

Allgemeine Hinweise:

- Das Handbuch muss von allen Benutzern gelesen werden und jederzeit zugänglich sein
- Die Montage, Inbetriebnahme und Bedienung darf nur von ausgebildetem und geschultem Personal erfolgen
- Die Sicherheitshinweise und das Handbuch sind von allen Personen zu beachten, die mit dem Gerät arbeiten
- Beim Einsatzort des Geräts müssen die geltenden Regeln und Vorschriften zur Unfallverhütung beachtet werden
- Das Handbuch enthält die wichtigsten Hinweise, um das Gerät sicherheitsgerecht zu betreiben
- Um einen sicheren und ordnungsgemäßen Betrieb des Geräts zu gewährleisten, wird eine sachgerechte Lagerung, sachgemäßer Transport, Aufstellung und Inbetriebnahme sowie sorgfältige Bedienung vorausgesetzt

Hinweis:
Für die im Handbuch beschriebenen Einstellungen und Features, ist nur eine ads-tec Original Firmware / Software zulässig. Durch aufspielen einer nicht durch ads-tec freigegeben Firmware / Software erlischt die Gewährleistung.

2.1 SICHERHEITSHINWEISE

Achtung:
Das Anschließen von Leitungen (Stromversorgung, Schnittstellenkabel) darf nur im abgeschalteten Zustand erfolgen um Beschädigungen am Gerät zu vermeiden.

Achtung:
Montagearbeiten am Gerät sind nur unter gesichertem und spannungsfreien Zustand erlaubt.

Hinweis:
Achten Sie bei der Handhabung elektrostatisch gefährdeter Bauteile auf die relevanten Sicherheitsmaßnahmen.
(DIN EN 61340-5-1 / DIN EN 61340-5-2)

2.2 BETRIEBSORT

Das Gerät ist für den industriellen Einsatz konzipiert. Es ist darauf zu achten, dass die spezifizierten Umweltbedingungen eingehalten werden. Der Einsatz in nicht spezifizierter Umgebung z. B. auf Schiffen, im EX-Bereich oder in extremer Höhe ist untersagt.

Achtung:

Um Kondensatbildung zu vermeiden darf das Gerät erst eingeschaltet werden, nachdem es sich der vorgeschriebenen Umgebungstemperatur angeglichen hat. Dasselbe gilt, wenn das Gerät extremen Temperaturschwankungen ausgesetzt wurde.

Überhitzung im Betrieb verhindern: Das Gerät darf keiner direkten Bestrahlung durch Sonnenlicht oder anderen Licht- oder Wärmequellen ausgesetzt werden.

Achtung:

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Achtung:

Wird das Gerät im Außenbereich eingesetzt, muss sich im Fangbereich ein Blitzableiter befinden. Es muss sichergestellt werden, dass alle von außen eingeführten leitfähigen Systeme einen Blitzschutz-Potenzialausgleich besitzen.

2.3 SCHÄDEN DURCH UNSACHGEMÄßEN GEBRAUCH

Weist das Bediensystem offensichtliche Schäden auf, verursacht durch z.B. falsche Betriebs-/ Lagerbedingungen oder unsachgemäße Handhabung, so ist das Gerät umgehend stillzulegen und gegen unbeabsichtigte Inbetriebnahme zu schützen.

2.4 GEWÄHRLEISTUNG / REPARATUR

Während der Gewährleistungszeit dürfen Reparaturen nur vom Hersteller oder durch vom Hersteller autorisierte Personen durchgeführt werden.

2.5 ALLGEMEINE HINWEISE ZUR 5GHZ VERSION (802.11 A / 802.11 H) ETSI

- Das Gerät ist für die Verwendung von Kanälen des 5 GHz Bandes nach ETSI EN 301 893 V1.3.1 zertifiziert. Dabei ist für den Benutzer folgendes zu beachten:
- Access Point und auch Access Client Geräte verwenden DFS und TPC standardmäßig auf allen 5 GHz Kanälen, sowoh bei Indoor- wie Outdoor-Konfiguration. Die Geräte können deshalb immer mit 23 dBm bzw. 30 dBm maximaler Abstrahlleistung betrieben werden.

Hinweis:

Access Points dürfen DFS im Außenbereich nicht abschalten. Ein Access Client darf das DFS abschalten. Diese Einstellung ist standardmäßig abgeschaltet.

- 802.11a Kanäle lassen sich nicht fix einstellen.

Hinweis:

Die unteren 4 Kanäle (non-DFS) lassen sich fix einstellen, wenn DFS abgeschaltet ist. Das Abschalten des DFS hat jedoch zur Folge das die Funktionen 60s Scan und Radar Detection auch abgeschaltet sind.

- Beim Aktivieren des AccessPoints wird dieser einen initialen Radardetektionsscan durchführen und dabei 60 Sekunden lang auf einem zufällig frei gewählten Kanal auf einen Radarimpuls warten, bevor der Betrieb auf diesem Kanal gestartet wird.
- Wird während des Betriebs ein Radarimpuls von einem Access Client detektiert wird dies dem Access Point nach 8011.h gemeldet. Der Access Point wechselt darauf hin oder aufgrund einer eigenen Detektion mit einem Channel Switch nach 802.11h den Kanal. Der Verbindungsausfall beträgt normalerweise weniger als 80ms.
- Die Maximal Zulässige Abstrahlleistung ist je nach Kanal verschieden. Daher ist es notwendig, dass der Benutzer eine korrekte Einstellung der Antennenverstärkung vornimmt, wenn die Standardantenne ausgetauscht wird!

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

2.6 ANTENNENÜBERSICHT FÜR DEN EINSATZ IN USA UND CANADA / FCC

ANTENNA LIST FOR USE IN USA AND CANADA / FCC

- This antenna types can be used with the Access Points and Access Client in USA and Canada. The antennas can be ordered at ads-tec GmbH. For the correct operation you have to use an absorbability cabel for the different antenna types.

Ads-tec part number	Ads-tec part description	Antenna type	Frequency band	Gain	absorbability
DZ-PCKO-11032-0	RAP Antenne 2,4 GHz SMA-R 5dBi	Swivel	2,4 ~ 2,4835 GHz	5 dBi	none
DZ-PCKO-11033-0	RAP Antenne 5 GHz SMA-R 7dBi	Swivel	5,1 ~ 5,835 GHz	7 dBi	none
DZ-PCKO-11034-0	RAP Antenne 2,4 GHz N-fem. 9 dBi	Omni	2,4 ~ 2,4835 GHz	9 dBi	none
DZ-PCKO-11034-1	RAP Antenne 2,4 GHz N-fem. 12 dBi	Omni	2,4 ~ 2,4835 GHz	12 dBi	none
DZ-PCKO-11035-0	RAP Antenne 2,4 GHz N-fem. 12 dBi	Panel	2,4 ~ 2,4835 GHz	12 dBi	none
DZ-PCKO-11035-1	RAP Antenne 2,4 GHz N-fem. 18 dBi	Panel	2,4 ~ 2,4835 GHz	18 dBi	minimum 20m (it is a Ecoflex10*1 cable to use)
DZ-PCKO-11036-0	RAP Antenne 5 GHz N-fem. 12 dBi	Omni	5,1 ~ 5,835 GHz	12 dBi	minimum 14m (it is a Ecoflex10*1 cable to use)
DZ-PCKO-11037-0	RAP Antenne 5 GHz N-fem. 12 dBi	Panel	5,1 ~ 5,835 GHz	12 dBi	minimum 20m (it is a Ecoflex10*1 cable to use)
DZ-PCKO-11037-1	RAP Antenne 5 GHz N-fem. 20 dBi	Panel	5,1 ~ 5,835 GHz	20 dBi	minimum 37m (it is a Ecoflex10*1 cable to use)

*1 It has at 2,4GHz 22.5dB/100m absorbability and at 5GHz 35.9dB/100m absorbability. Additional every plug has 0.5dB absorbability.

Warning:

Behalf of the correct operation you have use an absorbability element for the different antenna types.

Note:

Also light wave conductor cable can be used. It is necessary to use terminating impedance for the correct use.

2.7 KANALÜBERSICHT FÜR DEN EINSATZ IN USA UND CANADA / FCC

CHANNEL LIST FOR USE IN USA AND CANADA / FCC

- The following List showes the pool of available frequency and channles for the use in USA and Canada. The customer can define between Indoor and Outdoor use. This option can be selected by a checkbox in the web interface.

Frequency	Channel	Indoor use	Outdoor use
2,4 GHz (2.400~2.483GHz)	1 – 11	X	X
5 GHz (5.18~5.24GHz)	36,40,42,44,48	X	
5 GHz (5.725~5.825GHz)	149 ,153,157,161,165	X	
5 GHz (5.725~5.825GHz)	149 ,153,157,161,165		X

2.8 WLAN HINWEISE

Achtung:

Diese Hinweise müssen beim Betrieb der Geräte berücksichtigt werden:

- *Das Gerät bietet kein „sicheres“ Übertragungsmedium*
- *Mit den Geräten können keine Real-Time Systeme aufgebaut werden*
- *Die Geräte verfügen über kein deterministisches Systemverhalten*
- *Es wird keine MIN/MAX Roamingzeit gewährleistet*

Die Einstellung der gültigen Regulierungsbehörde und der Antennenverstärkung liegt in der Verantwortung des Betreibers

3 EINLEITUNG

Zuverlässig, robust und sicher im wireless LAN: Auf Basis neuester Technologien ist der Industrie Rugged Access Point (RAP) die Netzwerkschnittstelle für Anwendungen im Bereich Kommissionierung, mobile computing und Datenkommunikation. Der RAP unterstützt alle Standards wie 802.11 a/b/g bei einer Sendefrequenz von 2,4 und 5 GHz. Robuste Technik ist im Industrieumfeld eine Selbstverständlichkeit. Egal, ob sie das Gerät im Kühlhaus oder unter großer Hitze einsetzen möchten, der erweiterte Temperaturbereich macht es möglich. Durch die MIL-Zertifizierung ist der RAP außerdem mit einem der härtesten Vibrations- und Schocktests zertifiziert und garantiert damit absolute Robustheit.

Hinweis:

Die in dieser Dokumentation enthalten Hyperlinks, welche zu externen Webseiten führen, können aufgrund von Aktualisierungen nicht mehr funktionieren oder unter einem anderen Hyperlink erreichbar sein. Die ads-tec GmbH (nachstehend „ads-tec“) übernimmt keine Garantie oder Haftung dahingehend, dass Hyperlinks zu externen Webseiten funktionieren. Ferner übernimmt ads-tec keine Garantie oder Haftung jeglicher Art im Hinblick auf die Installation, Anwendung und der Fehlerfreiheit sämtlicher Open-Source Software.

Hinweis:

Zur effizienten Online-Konfiguration Ihrer ads-tec Geräte kann die aktuellste Version des kostenlosen Tools „**IDA light**“ auf der Unternehmenshomepage **http://www.ads-tec.de** heruntergeladen werden. Durch das Tool haben Sie z.B. die Möglichkeit, einzelne Parameter oder ganze Parametergruppen an einem Mastergerät zu definieren und diese an eine begrenzte Auswahl bzw. an alle ads-tec-Geräte gleicher Bauart und Version zu übertragen, ohne diese Konfigurationen zeitaufwendig an jedem einzelnen Gerät vornehmen zu müssen. U.a. haben Sie die Möglichkeit, mit wenigen Handgriffen fortlaufende IP-Adressen für Ihre ads-tec-Geräte zuzuweisen.

Mit IDA light können Sie bequem eigene Parametergruppen nach Ihren spezifischen Anforderungen erstellen und diese jederzeit modifizieren.

Hinweis:

Wenn in der Dokumentation nicht explizit von Access Client die Rede ist, sind immer Access Point und Access Client gemeint.

3.1 AUSSTATTUNGSVARIANTEN

		RAP – Rugged Access Point											
		RAP1000 Serie											
		RAP 1110	RAP 1111	RAP 1210	RAP 1211	RAP 1120	RAP 1121	RAP 1220	RAP 1221	RAP 1510	RAP 1511	RAP 1520	RAP 1521
Funkmodule	1 WLAN Modul	x	x	x	x					x	x		
	2 WLAN Module					x	x	x	x			x	x
Ports	1x Cu-RJ45 Port	x	x			x	x			x	x	x	x
	4x Cu-RJ45 Port (switch)									x	x	x	x
	1x Glasfaser Ethernet Port			x	x			x	x				
Spannungs-versorgung	24 V DC	x	x	x	x	x	x	x	x	x	x	x	x
	110/230 V AC integriert		x		x		x		x		x		x
	Redundant e Spannungsversorgung	x	x		x	x	x		x	x	x	x	x
Client Modus	RAP incl. Client - Modus	x	x	x	x	x	x	x	x	x	x	x	x
	Seamless Roaming Client*					x	x	x	x			x	x

		RAC – Rugged Access Client					
		RAC1000 series				RAC2000 series	
		RAC 1120	RAC 1121	RAC 1220	RAC 1221	RAC 2110	RAC 2120
Funkmodule	1 WLAN Modul					x	
	2 WLAN Module	x	x	x	x		x
Ports	1x Cu-RJ45 Port	x	x			x	x
	4x Cu-RJ45 Port (Switch)						
	1x Ethernet port			x	x		
Spannungsversorgung	24 V DC	x	x	x	x	x**	x**
	110/230 V AC integriert		x		x		
	Redundante Spannungsversorgung	x	x		x		
Client Modus	RAP incl. Client Modus						
	Seamless Roaming Client*	x	x	x	x		x

* Seamless Roaming Clients: Von Access Point zu Access Point ohne jeglichen Paketverlust oder Unterbrechung der Datenverbindung
**12 – 24V

RJ45 (Registered Jack 45 = genormte Buchse) ist ein Ethernet-Standard wie er häufig in der Telekommunikationswelt verwendet wird. Die Übertragungsart entspricht 10/100Mbits half & full DUPLEX 100 BASE-TX.

LWL (Lichtwellenleiter) sind flexible optische Medien in denen Licht kontrolliert geleitet werden kann. Die Lichtwellenleiter-Technologie ist im Gegensatz zum Ethernet-Standard gegen Spannungsstörungen unempfindlich.

Der zu verwendende Steckertyp entspricht dem MTRJ-Standard Multimode mit der Übertragungsart 100Base-FX 100 Mbit⁄s Ethernet über Glasfaser.

3.2 LIEFERUMFANG

Der Inhalt der Verpackung muss auf Vollständigkeit überprüft werden:

- 1 Gerät
- 1 x 2 pol. COMBICON Stecker bei 24V DC Geräten
  Hersteller: Phoenix Contact
  Artikelbezeichnung: FMC 1,5 / 2-STF-3,5
- 1 x 3 pol. COMBICON Stecker bei 230V AC Geräten
  Hersteller: Phoenix Contact
  Artikelbezeichnung: MC 1,5 / 3-ST1F-5,08
- Vier oder acht Antennen (je nach Ausstattung)
- Durchführungstüllen / Blindstopfen
- Montagekit mit Montageplatte und Befestigungsmaterial (am Gerät montiert)
- Quick Install Guide / Quick Montage Guide
- GNU General Public License
- Service CD

3.3 UMWELTBEDINGUNGEN

Das Gerät kann unter folgenden Bedingungen betrieben werden. Werden diese Angaben nicht eingehalten, erlischt die Gewährleistung des Geräts. Für Schäden, die durch falsche Handhabung entstehen, haftet ads-tec nicht.

- Umgebungstemperatur
  im Betrieb -20 … 55° C
  bei Lagerung -20 … 55° C
- Feuchte
  im Betrieb 10 … 85% ohne Kondensat
  bei Lagerung 10 … 85% ohne Kondensat
- Vibration
  im Betrieb 1 G, 10 … 500 Hz
  (DIN EN 60068-2-6)

  Vibrationsprüfung: MIL-STD-810F 514.5 C-2
  5 … 500 Hz (01-01-2000)
- Schock
  im Betrieb 5 G, bei einer Halbwelle von 30 ms
  (DIN EN 60068-2-29)

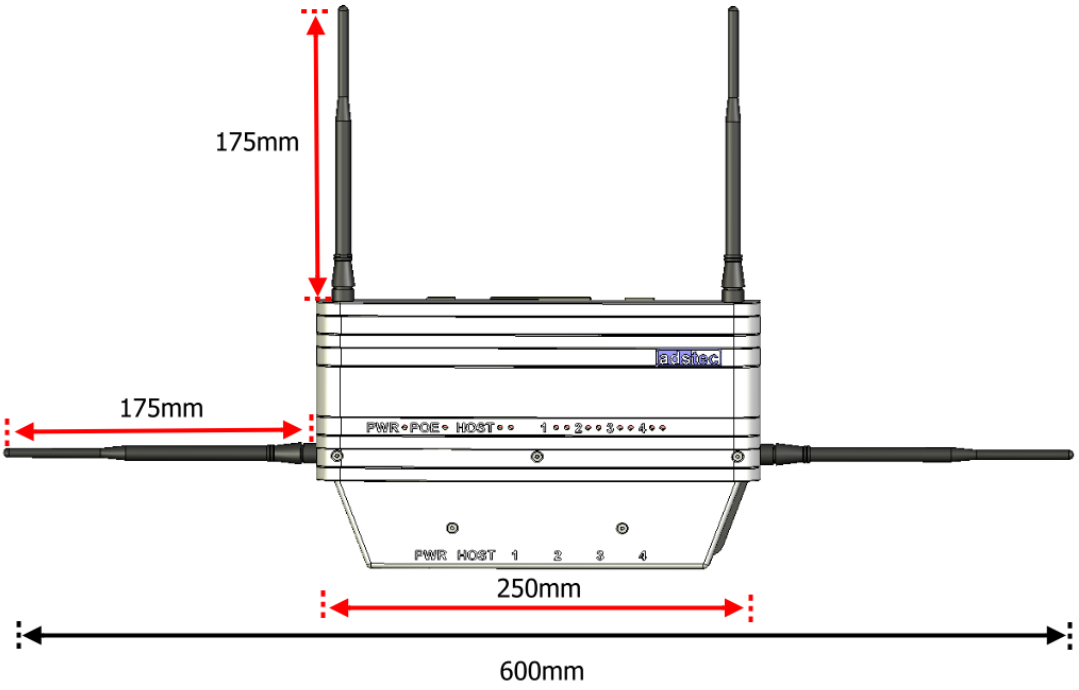
4 MONTAGE

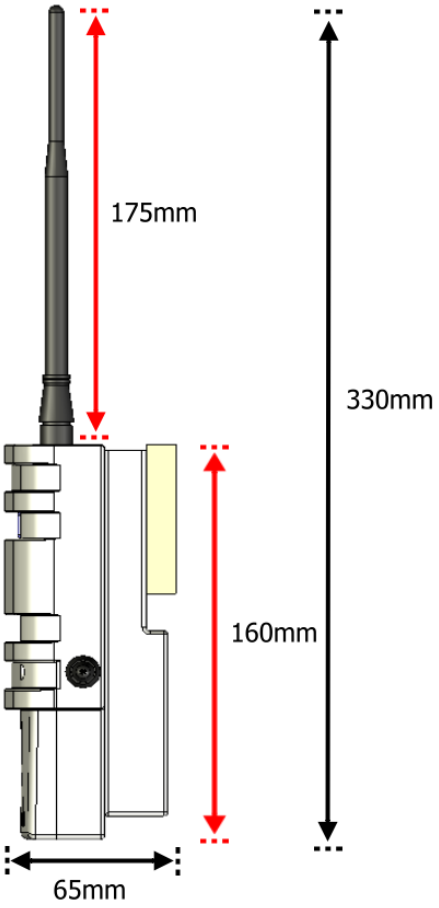
4.1 MONTAGEMÖGLICHKEIT

Das Gerät ist für den industriellen Einsatz vorgesehen und kann überall dort eingesetzt werden, wo die Umweltbedingungen nicht verletzt werden. Aus Gründen der Montage und des Betriebs sollte das Gerät möglichst an einer Stelle angebracht werden, an der das WLAN Netz nicht beeinträchtigt wird. Das WLAN Netz wird vor allem durch Eisenträger und dicke Betonwände beeinträchtigt.

4.2 AUßENABMESSUNGEN DES GERÄTS

Höhe: 160 mm (ohne Antenne)
Breite: 250 mm (ohne Antenne)
Tiefe: 65 mm (ohne Antenne)



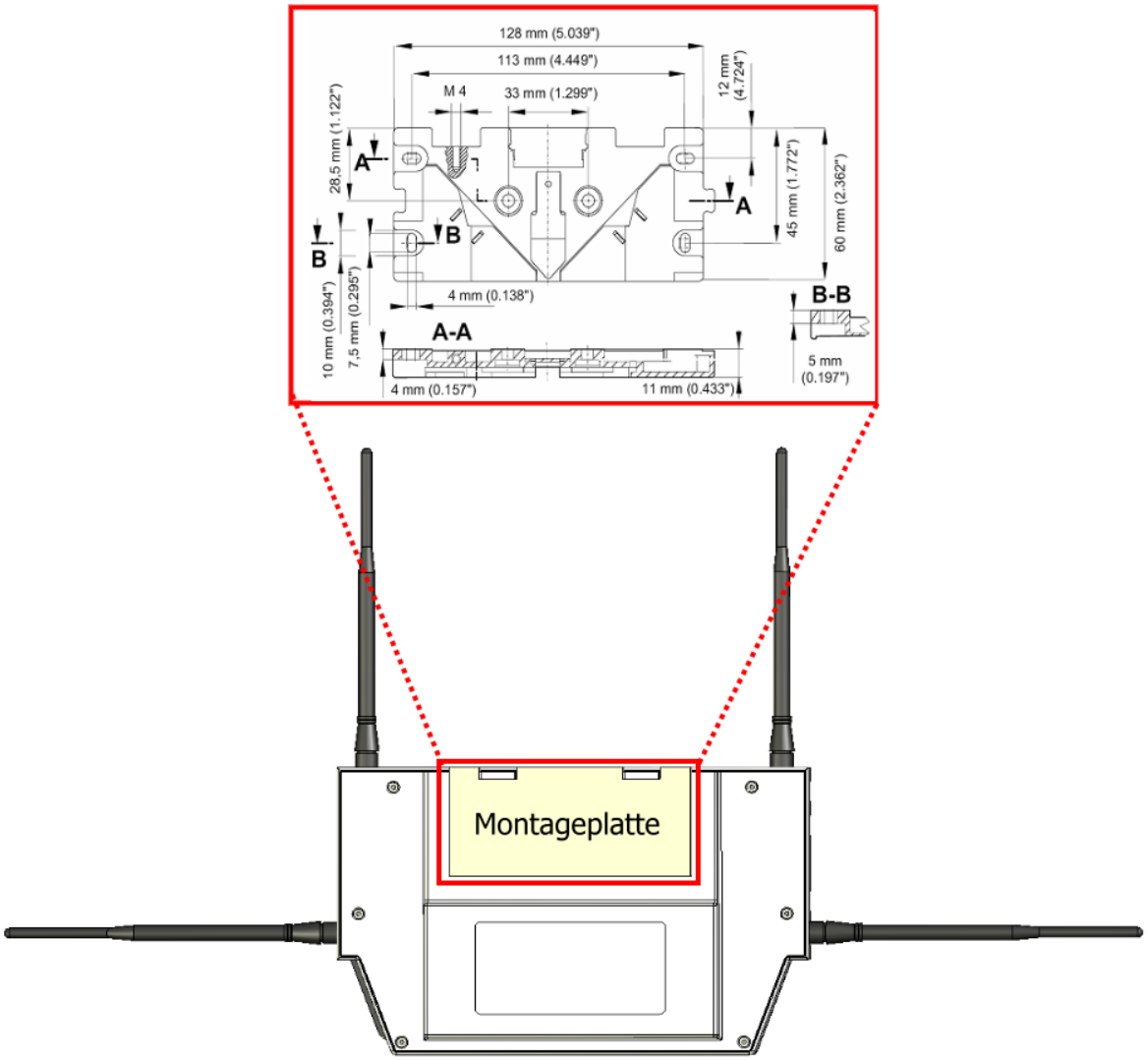

175mm
330mm
160mm
65mm

4.3 MONTAGESKIZZE DES GERÄTES

Hinweis:

Die hier abgebildete Montageskizze ist keine 1:1 Ansicht.

Die 1:1 Abbildung entnehmen Sie bitte dem Abschnitt Quick Install Guide Montage.

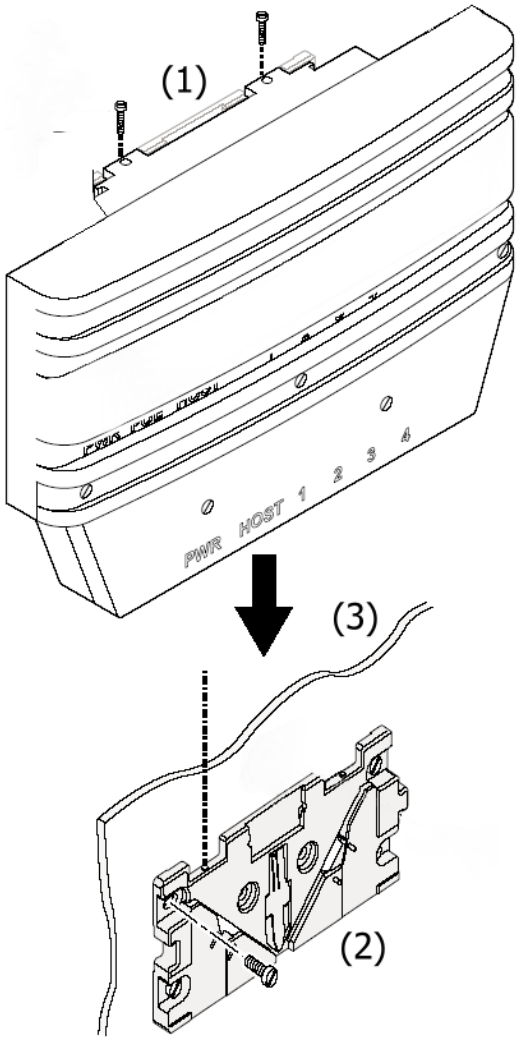


4.4 BEFESTIGUNG DES GERÄTS

Die Montageplatte ist im Auslieferungszustand bereits am Gerät montiert.

1) Um das Gerät an einer von Ihnen ausgewählten Position zu montieren, lösen Sie die Inbusschrauben (M4x12).**(1)**

2) Befestigen Sie die Montageplatte ohne Gerät an der von Ihnen ausgewählten Position. Sorgen Sie dafür, dass die Montageplatte von mindestens zwei gegenüberliegenden Schrauben gehalten wird. **(2)**



3) Setzen Sie das Gerät auf die montierte Halterung und stellen Sie sicher, dass Gerät und Halterung bündig abschließen. **(3)**

4) Sichern Sie das Gerät an der Halterung mit den zuvor entfernten Inbusschrauben. **(1)**

Hinweis:

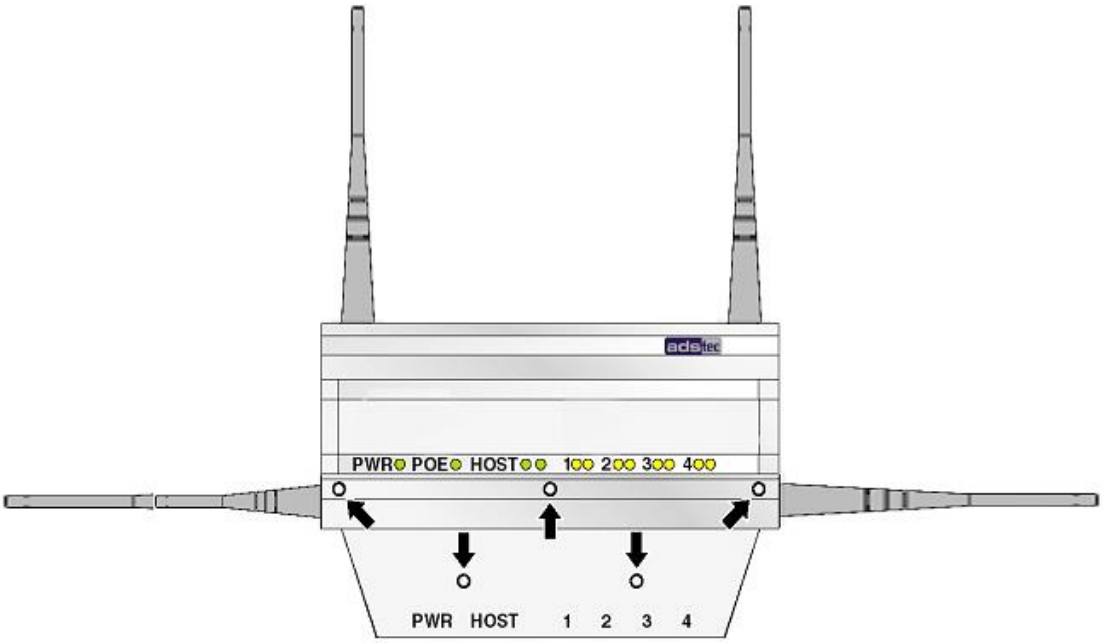
Bitte beachten Sie, dass das Gerät nicht hinter oder neben einem Gegenstand montiert wird, da dadurch die Empfangs- und Sendeleistung beeinträchtigt werden kann.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

4.5 ANSCHLUSS DER VERSORGUNGSLEITUNGEN

Der Versorgungsanschluss sowie die Schnittstellen des Geräts sind im Inneren des Gehäuses untergebracht. Um die Versorgungsleitung oder die Schnittstellenkabel anschließen zu können, muss der Serviceschachtdeckel des Gehäuses abgenommen werden.

Bitte entfernen Sie die fünf gekennzeichneten Schrauben (M3x8).



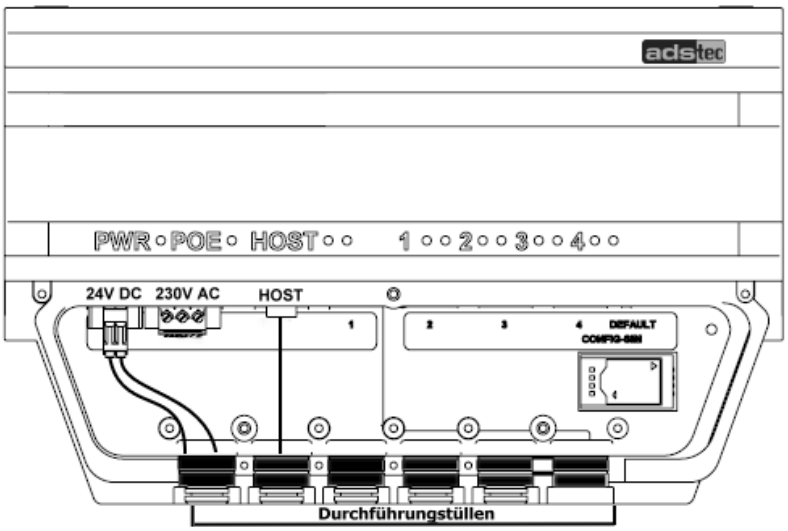
Achtung:

Um Schäden an der Elektronik zu vermeiden, muss das Gerät ausgeschaltet werden, bevor Steckverbindungen hergestellt oder gelöst werden!

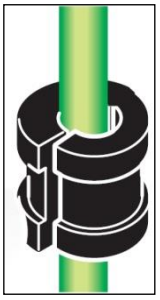
Für das Gerät zugelassene Spannung beachten.

Nachdem der Serviceschachtdeckel entfernt wurde, können die Anschlussleitungen installiert werden.

Die Darstellung zeigt eine Beispielinstallation eines Gerätes mit 24V DC Spannungsversorgung und angeschlossener Hostleitung.



Für die Sicherstellung der IP65 Schutzart müssen die Anschlussleitungen mit den passenden Durchführungstüllen versehen werden.



Hinweis:

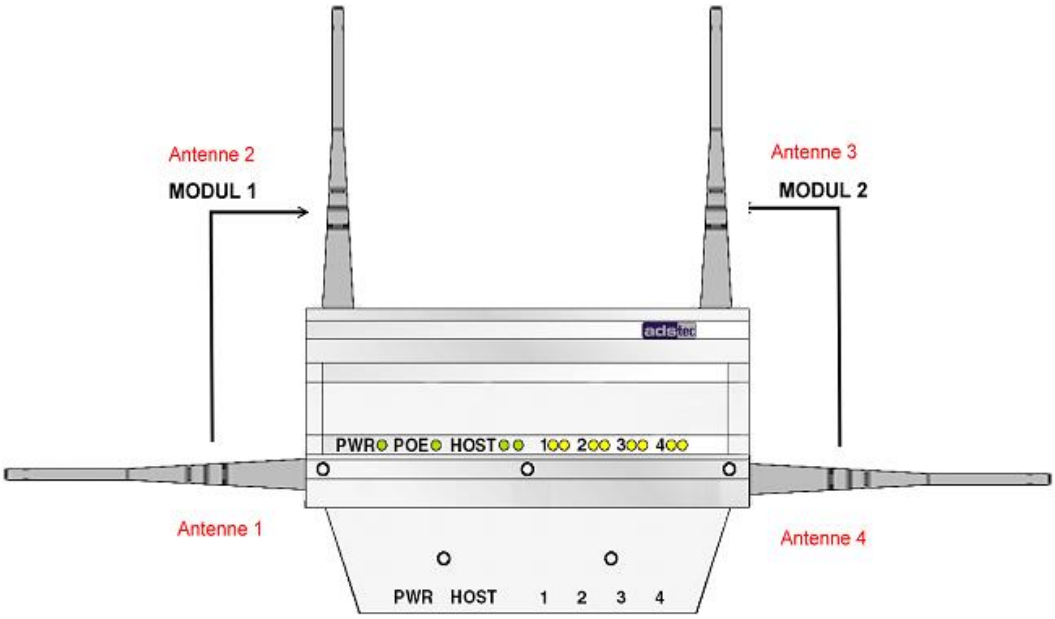
Die Größe der Durchführungstüllen muss zum passenden Durchmesser der Leitungen ausgewählt werden.

Nachdem Sie die Durchführungstüllen um die Leitungen gelegt haben, müssen sie noch in die vorgesehenen Mulden eingelegt werden.

Zum Schluss setzen Sie den Serviceschachtdeckel wieder auf das Gerät und verschrauben ihn mit den fünf zuvor gelösten Schrauben.

4.6 MONTAGE DER ANTENNEN

Für den Betrieb eines WLAN-Moduls sollten 2 Antennen montiert werden.



Je nach Geräteausstattung ist das Gerät in der Lage zwei Funkmodule für zwei verschiedene WLAN-Netze parallel zu betreiben. Die korrekte Antennenmontage für ein Modul besteht aus einer horizontal und einer vertikal ausgerichteten Antenne. Die vier oder acht mitgelieferten Antennen arbeiten auf den Frequenzbereichen 2.4GHz oder 5GHz (je zwei oder vier).

Schrauben Sie die Antennen auf die dafür vorgesehenen Gewinde.

5 SYSTEMMERKMALE

5.1 ALLGEMEINE LED STATUS-ANZEIGEN

Über die integrierten LEDs wird der Status der verschiedenen Schnittstellen angezeigt. Dadurch ist eine Status-Diagnose des Access Points/Clients am Einsatzort möglich. In der Übersicht werden die Status-Anzeigen des Geräts dargestellt.

LEGENDE

Status der LED	Darstellung in der Tabelle
Aus	
Grün	
grün blinkend	
Orange	
orange blinkend	

SPANNUNGSVERSORGUNG / POWER OVER ETHERNET / HOST / SWITCH

POWER	SIGNAL	AKTION
PWR		Das Gerät wird nicht mit Spannung versorgt.
PWR		Das Gerät wird über POWER mit Spannung versorgt und ist betriebsbereit.
POWER OVER ETHERNET		
POE		Das Gerät wird nicht mit einer Spannung über PoE versorgt.
POE		Das Gerät wird über PoE mit Spannung versorgt und ist betriebsbereit.
HOST		
LINKE LED LINK		Die Schnittstelle ist nicht mit einer Gegenstelle verbunden.
LINKE LED LINK		Die Schnittstelle ist mit einer Gegenstelle verbunden und ist betriebsbereit.
RECHTE LED ACT		Es findet kein Datenverkehr zwischen Gerät und Gegenstelle statt.
Rechte LED ACT		Zeigt den Datenverkehr zwischen Gerät und Gegenstelle an.

SWITCH 1 / 2 / 3 / 4		
LINKE LED LINK		Die Schnittstelle ist nicht mit einer Gegenstelle verbunden.
LINKE LED LINK		Die Schnittstelle ist mit einer Gegenstelle verbunden und ist betriebsbereit.
RECHTE LED ACT		Es findet kein Datenverkehr zwischen Gerät und Gegenstelle statt.
Rechte LED ACT		Zeigt den Datenverkehr zwischen Gerät und Gegenstelle an.

5.2 BETRIEBSBEDINGTE LED STATUS-ANZEIGEN

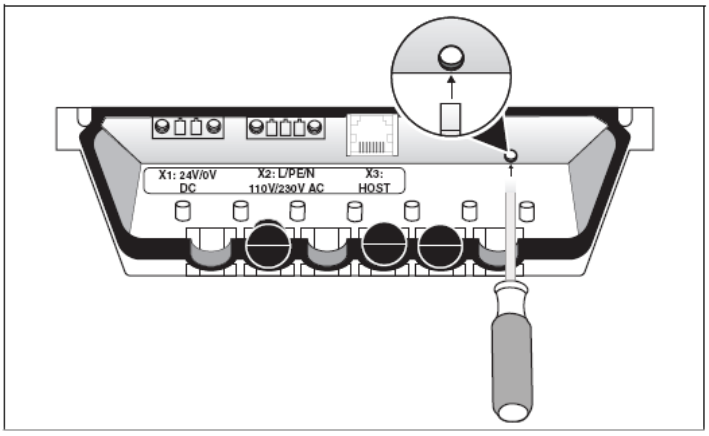
VERHALTEN DER STATUS ANZEIGEN BEIM BOOTVORGANG

Sobald der Access Point / Client mit einer Spannungsquelle versorgt wird, beginnt der Bootvorgang. Mit Hilfe der **HOST** LEDs kann überprüft werden ob das Gerät bootet. Anhand der folgenden Darstellung kann der korrekte Bootvorgang mittels der Blinkfrequenz der LEDs nachvollzogen werden. In diesem Beispiel ist kein **HOST** Kabel / PoE eingesteckt.

PWR	SIGNAL	AKTION
L+		Das Gerät wird über POWER mit Spannung versorgt und ist betriebsbereit.
POE		
L+		Das Gerät wird über BACKUP mit Spannung versorgt und ist betriebsbereit.
HOST		
LINK / ACT		LEDS BLINKEN EINMAL KURZ AUF
		LED BLINKT LANGSAM, DANACH SCHNELL (20X)
		LED GEHT AUS

VERHALTEN DER STATUS ANZEIGEN BEIM ZURÜCKSETZEN AUF DEFAULT-EINSTELLUNGEN

Über den Default-Setting Taster unter dem Schnittstellendeckel, kann jederzeit unabhängig von der Konfiguration, der Access Point / Client auf die Default-Einstellungen zurückgesetzt werden.



Um das Gerät auf die Default-Einstellungen zurückzusetzen, muss der Default-Setting Taster gedrückt und das Gerät dann eingeschaltet werden. Der Default-Setting Taster muss für ca. 20 Sekunden gedrückt werden. Sobald die linke HOST-LED konstant grün leuchtet kann der Taster wieder gelöst werden. In dem Beispiel ist kein **HOST** Kabel / PoE eingesteckt. Anhand der folgenden Darstellung kann der korrekte Factory- Default Vorgang anhand der Blinkfrequenz der LEDs nachvollzogen werden.

PWR	SIGNAL	AKTION
L+	■	Das Gerät wird über POWER mit Spannung versorgt und ist betriebsbereit.
POE		
L+	■	Das Gerät wird über BACKUP mit Spannung versorgt und ist betriebsbereit.
HOST		
LINK / ACT	■ ■	LEDS BLINKEN REGELMÄßIG
LINK / ACT	□ □	LEDS GEHEN AUS

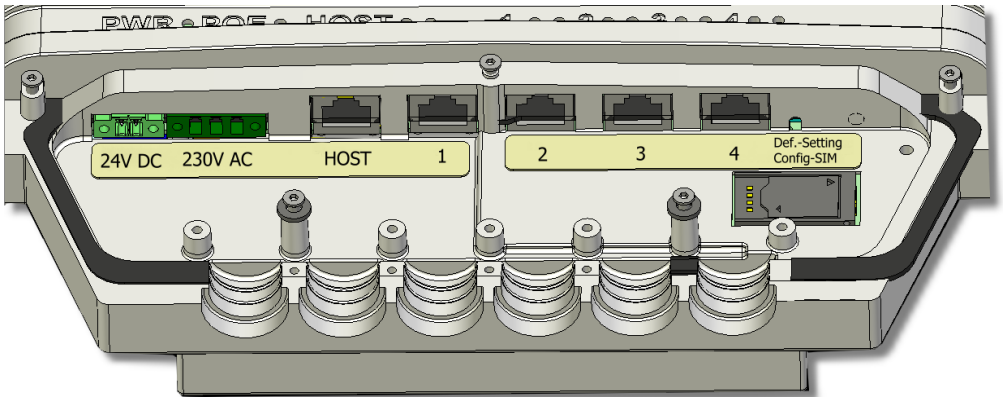
VERHALTEN DER STATUS ANZEIGEN BEIM FIRMWAREUPDATE

Über das Webinterface kann ein Firmware-Update durchgeführt werden. Der eigentliche Update-Vorgang kann einige Minuten in Anspruch nehmen. Anhand der folgenden Darstellung kann der korrekte Firmware-Update Vorgang anhand der Blinkfrequenz der LEDs nachvollzogen werden.

PWR	SIGNAL	AKTION
L+		Das Gerät wird über POWER mit Spannung versorgt und ist betriebsbereit.
POE		
L+		Das Gerät wird über BACKUP mit Spannung versorgt und ist betriebsbereit.
HOST		
LINK / ACT		LEDS BLINKEN SCHNELL
LINK / ACT		LINK GEHT AUS / ACT BLINKT
LINK / ACT		LINK LEUCHTET KONSTANT / ACT GEHT AUS
LINK / ACT		LINK LEUCHTET KONSTANT / ACT BLINKT LAMGSAM
LINK / ACT		LINK LEUCHTET KONSTANT / ACT BLINKT SCHNELL
LINK / ACT		LINK LEUCHTET KONSTANT / ACT GEHT AUS
ANSCHLIEßEND KANN DAS WEBINTERFACE ÜBER „VERSUCHE NEU ZU VERBINDEN“ GESTARTET WERDEN		

5.3 SCHNITTSTELLENÜBERSICHT

Die folgende Darstellung zeigt die Verfügbaren Schnittstellen des Gerätes. Je nach Ausstattungsoption kann es zu Unterschieden kommen.



Das Gerät hat folgende Schnittstellen:

1. Power 24V DC Spannungsversorgung (2pol. COMBICON Stecker)
2. Power 230V AC Spannungsversorgung (3pol. COMBICON Stecker)
3. HOST RJ45 (PoE) oder LWL- Anschluss
4. SWITCH 4x RJ45-Anschluss (optional bei Access Client)
5. Default-Setting Taster
6. SIM Karten Reader

Hinweis:
Alle Eingangsspannungen können redundant angeschlossen werden (Power 24V DC, Power 230V AC und PoE über HOST).

SPANNUNGSVERSORGUNG 24V DC

Die Versorgungsspannung wird über eine Durchführungsklemme mit Schraubanschluss zugeführt (Bild zeigt Buchse im Gerät).

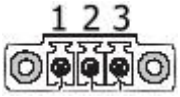
PIN-NUMMER	SIGNAL NAME
1	24V DC
2	0V DC

PIN 1: = L+ 24V DC Spannungsversorgung
PIN 2: = GND Ground

SPANNUNGSVERSORGUNG 110/230 VAC

Die Versorgungsspannung wird über eine Durchführungsklemme mit Schraub anschluss zugeführt. (Bild zeigt Buchse im Gerät)

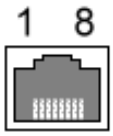
PIN-NUMMER	SIGNAL NAME
1	110/230 V AC
2	PE
3	0 V DC



SPANNUNGSVERSORGUNG PoE / HOST (IEEE 802.AF)

Für die Übertragung der Stromversorgung wird das Adapterpaar 4/5 für den Pluspol und das Adernpaar 7/8 für den Minuspol verwendet.

PIN-NUMMER	SIGNAL NAME
1	TX +
2	TX -
3	RX +
4	PoE/G
5	PoE/G
6	RX -
7	PoE/-48V
8	PoE/-48V



Hinweis:

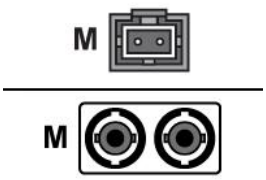
Die Übertragung der 48 VDC Spannung ist für maximal 100 Meter ausgelegt. Diese ist auf das Ethernet abgestimmt. Die angeschlossenen Geräte dürfen 350 mA Strom abnehmen und die maximale Speiseleistung beträgt 15,4 Watt.

Bei Netzwerken mit Hubs oder Switches müssen diese PoE tauglich sein, damit die Stromversorgung erfolgen kann.

LWL-ETHERNET

Bei dem LWL Anschluss wird ein MTRJ Glasfaserstecker verwendet.

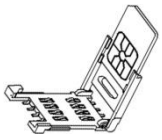
Multimode Kabel von MTRJ-Stecker nach Duplex Stecker 62.5/125µm.

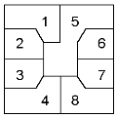


SIM CARD READER NACH ISO 7816

Der SIM-Card Reader dient der Speicherung von Konfigurationsdaten.

PIN-NUMMER	SIGNAL NAME
1	VCC 5 Volt
2	RESET
3	CLOCK
4	n/c
5	GND
6	n/c
7	I/O
8	n/c





Hinweis:

Die Schnittstellen- sowie der Versorgungsstecker des Geräts sind an der Unterseite des Geräts angebracht. Die Stecker sollten gegen Herausrutschen gesichert werden.

6 INBETRIEBNAHME

6.1 ERST-KONFIGURATION

Achtung:

Die Erst-Konfiguration des Geräts kann nur über die mit HOST gekennzeichnete RJ45-/LWL Schnittstelle erfolgen.

FÜR DIE ERSTKONFIGURATION WIRD EIN RJ45 PATCHKABEL BENÖTIGT.

Anschluss der Spannungsquelle 24V DC / PoE

Das Gerät kann über eine **24V DC (2pol. Stecker)** Spannungsquelle, eine 230V AC (3pol. Stecker) oder über eine **PoE- Verbindung** versorgt werden. Die entsprechenden COMBICON Stecker sind im Lieferumfang enthalten.

Verbinden Sie das Gerät mit der geeigneten Spannungsquelle.

Anschluss des RJ45 / LWL Netzwerkkabels

Für die Erstinbetriebnahme des Gerätes ist zwingend eine Verbindung zwischen dem Gerät und einem PC über ein RJ45/LWL Netzwerkkabel notwendig.

Verbinden Sie das Gerät mit einem PC:

Geräte- HOST <-> PC-LAN-Anschluss

6.2 MANUELLE KONFIGURATION DES NETZWERKADAPTERS ÜBER DAS RJ45/LWL-KABEL

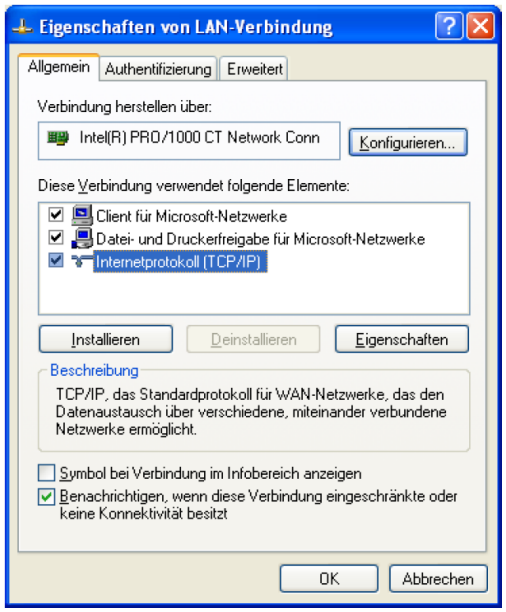
Hinweis:

Die nachfolgend beschriebenen Hinweise wurden mit Windows XP® erstellt. Sollten Sie ein anderes Betriebssystem nutzen, können die hier beschriebenen Pfade und Eigenschaften variieren.

Öffnen Sie nun die Eigenschaften-Karte ihres Netzwerkadapters. Der Pfad lautet:

Start> **Einstellungen**> **Netzwerkverbindungen**> **LAN-Verbindung**> **Eigenschaften**.

Im hier erscheinenden Dialog markieren Sie die Option: **Internetprotokoll (TCP/IP)** und klicken auf **Eigenschaften**



Markieren Sie nun den Punkt: **Folgende IP-Adresse verwenden**

Der Zugriff auf das Gerät wird erst ermöglicht, wenn die folgenden Parameter als fixe IP-Adresse eingetragen wurden oder sich der Rechner im selben Subnetzraum befindet:

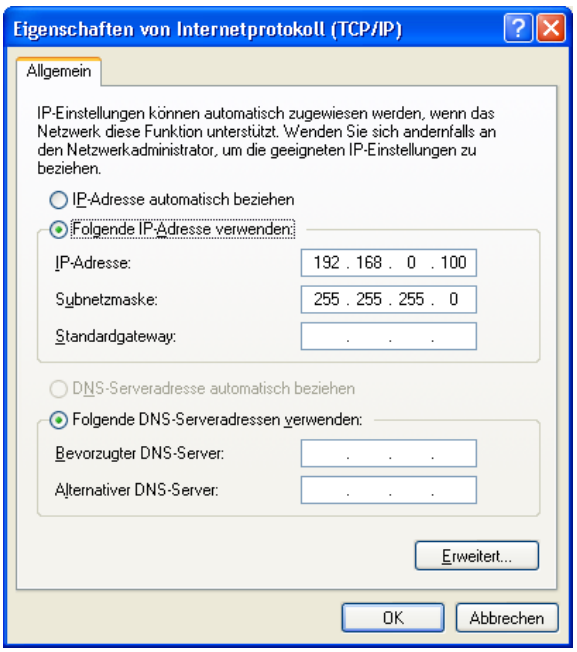
IP-ADRESSE: 192.168.0.100

Hinweis:

(Die letzte Ziffernfolge muss eine Zahl zwischen 1 und 253 sein, im Beispiel ist der Wert „**100**“ gewählt)

Nachdem die IP-Adresse eingetragen wurde, muss die **Subnetzmaske- Adresse** eingetragen werden. Wird in das Feld **Subnetzmaske** geklickt, wird automatisch die richtige Adresse eingetragen.

SUBNETZMASKE: 255.255.255.0


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 0 . 100
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway:
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Die Dialoge können nun mit **„OK“** geschlossen werden.

6.3 KONFIGURATION DES WLAN-NETZWERKADAPTERS

Um den WLAN-Netzwerkadapter zu konfigurieren, gehen Sie genauso vor wie bei der Konfiguration des Netzwerkadapters, mit der Ausnahme, dass die IP-Adresse nicht identisch sein darf.

IP-ADRESSE: 192.168.0.200

Hinweis:
(Die letzte Ziffernfolge muss eine Zahl zwischen 1 und 253 enthalten, im Beispiel ist der Wert „**200**“ gewählt)

ÖFFNEN DES GERÄTE WEBINTERFACES

Um das Webinterface des Geräts zu öffnen, starten Sie ihren Web-Browser. In die Adresszeile des Browsers geben Sie nun folgende IP-Adresse ein und bestätigen mit **„Enter“**.

HTTP://192.168.0.254

Login

Nach erfolgreicher Eingabe der IP-Adresse erscheint die Login-Eingabeaufforderung. In der Login-Eingabeaufforderung sind die Default-Einstellungen einzugeben.

Die Default-Konfiguration im Auslieferungszustand lautet:

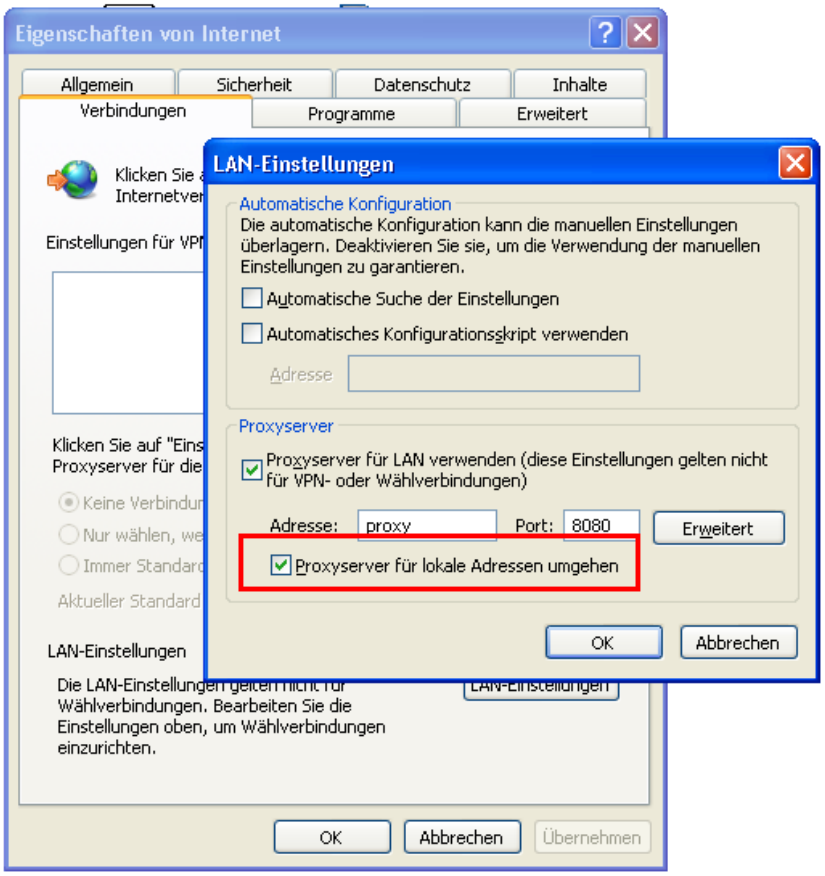
BENUTZERNAME : admin

PASSWORT : admin

Bestätigen Sie ihre Eingabe mit **OK**. Im Anschluss erscheint das Webinterface des Geräts.

Hinweis:

Wenn die Login-Eingabeaufforderung nicht erscheint, ist zu prüfen ob die Geräte über ein RJ45 Kabel verbunden sind. Ansonsten Verbinden Sie das Gerät mit einem PC.(Geräte Host Anschluss <> PC LAN – Anschluss)



6.4 ERSTKONFIGURATION IM GERÄTE-WEBINTERFACE

AKTIVIERUNG DES WLAN MODULS

Zum Aktivieren des/der WLAN Module müssen Sie auf folgende Webinterfaceseite wechseln:

GRUNDEINSTELLUNGEN>SCHNITTSTELLEN>WLAN 1/2

Je nach Ausstattungsoption des Gerätes stehen ein oder zwei WLAN Module zur Verfügung. Aktivieren Sie das gewünschte WLAN Modul durch Anhaken von **Aktiviere Schnittstelle** im Webinterface.

KONFIGURATION DES WLAN-MODULS:

Betriebsmodus:

Der Betriebsmodus des Geräts muss definiert werden. Zur Auswahl stehen: **ACCESS POINT** oder **Client**

Netzwerk Name (SSID)

Die SSID spiegelt den Namen des WLAN-Funknetzes wieder. Die Default-Einstellung lautet: **ads**

Die SSID kann frei benannt werden.

WLAN Modus:

Wählen Sie ihren bevorzugten WLAN Modus:

Achtung:

Verwenden Sie einen entsprechenden WLAN-Modus, der von Ihren WLAN-Teilnehmern unterstützt wird.

Regulierungsbehörde:

Wählen Sie ihren Standort aus.

Achtung:

Die Einstellung der gültigen Regulierungsbehörde und der Antennenverstärkung liegt in der Verantwortung des Betreibers.

Kanal:

Die Default–Einstellung lautet: **Auto**

Das Gerät wählt die beste Kanaleinstellung automatisch.

Speichern der Einstellungen:

Die von Ihnen getätigten Änderungen müssen nun noch aktiviert bzw. gespeichert werden. Klicken Sie dazu auf den Menüpunkt:

Konfiguration> Speichern.

Im nun erscheinenden Fenster klicken Sie auf **Speichern**. Die aktuelle Konfiguration wird nun übermittelt und gespeichert.

6.5 KONFIGURATION DES WLAN- NETZES

Öffnen Sie erneut die Eigenschaften Karte über den Pfad:

Start> **Einstellungen**> **Netzwerkverbindungen**. Navigieren Sie per Rechtsklick auf Ihre Funkverbindung und anschließend auf den Menüpunkt **Eigenschaften.** Klicken Sie nun auf den Reiter **Drahtlosnetzwerke**. Im nun erscheinenden Dialogfenster wählen Sie im Menüpunkt **bevorzugte Netzwerkverbindungen** den Button **Hinzufügen**. Geben Sie nun folgende Parameter an:

Netzwerk Name SSID: (frei gewählter Name des Funknetzes), ansonsten **ads** als Standard.

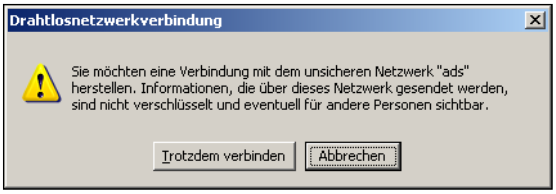
Netzwerk Authentifikation: Open

Verschlüsselung: Disabled

Die Dialogfenster können nun mit „**OK**“ geschlossen werden.

6.6 HERSTELLEN EINER VERBINDUNG MIT DEM DRAHTLOS-NETZWERK

Um eine Funkverbindung mit dem Gerät herzustellen, klicken Sie auf das WLAN Symbol in ihrer Taskleiste. In der erscheinenden Anzeige werden alle verfügbaren Netze angezeigt. Wählen Sie das Funknetz mit ihrer vergebenen SSID und klicken Sie auf **Verbinden**. Folgende Warnung erscheint:


Drahtlosnetzwerkverbindung
Sie möchten eine Verbindung mit dem unsicheren Netzwerk "ads" herstellen. Informationen, die über dieses Netzwerk gesendet werden, sind nicht verschlüsselt und eventuell für andere Personen sichtbar.
Trotzdem verbinden
Abbrechen

Um sich mit dem WLAN-Netz zu verbinden muss **„Trotzdem verbinden“** ausgewählt werden. Der Computer wird nun per Funk mit dem Gerät verbunden.

Hinweis:

Sollten Sie keine Verbindung zum Gerät aufbauen können, so empfehlen wir ein Rücksetzen des Geräts auf den Auslieferungszustand.

Hinweis:

Die momentane Konfiguration ist nicht verschlüsselt. Es wird empfohlen eine Verschlüsselung zu verwenden. Weitere Informationen zum Thema Verschlüsselung entnehmen Sie dem Kapitel Konfiguration>Sicherheit>WLAN 1/2.

7 ACCESS POINT SETUP-ASSISTENT

Für eine einfache und schnelle Inbetriebnahme sowie Konfiguration des Gerätes wurden zwei Assistenten integriert. Mit Hilfe des Setup-Assistenten ist eine geführte Konfiguration der Spracheinstellung, des Betriebsmodus sowie des Passwortes möglich. Über den Filter-Assistenten ist eine geführte Konfiguration der Filterregeln möglich. Weitere Informationen finden Sie im Kapitel Paket-Filter. Alle Einstellungen können auch unabhängig der Assistenten über die Weboberfläche geändert werden.

7.1 ERSTKONFIGURATION MIT HILFE DES SETUP-ASSISTENTEN

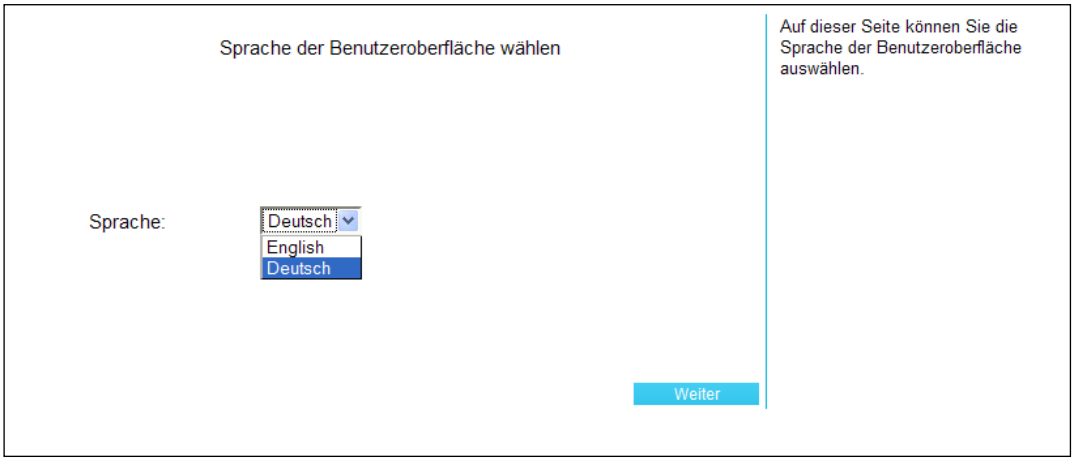
Um eine Basiskonfiguration durchzuführen, wählen Sie auf der Startseite im Feld **Quicklinks:**

STARTE SETUP ASSISTENT

Hinweis:

Das Fragezeichen rechts neben dem Drop-Down-Menü gibt Ihnen Hinweise und Kurzerklärungen zu den zur Auswahl stehenden Menüpunkten.

Die Hinweise und Kurzerklärungen werden mit dem Microsoft© Internet Explorer ab Version 7 und dem Mozilla Firefox© ab Version 1.0 korrekt dargestellt.

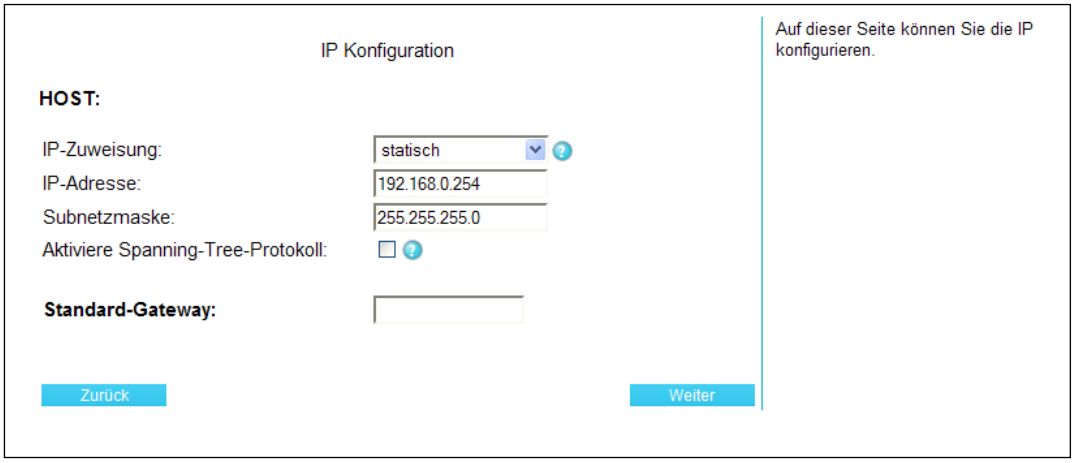


Diese führt Sie dann im Folgenden über das gesamte Webinterface.

Bestätigen Sie ihre Wahl mit: **Weiter**

7.1.1 IP-KONFIGURATION

Die IP-Konfiguration definiert das Verhalten der Host-Schnittstelle, welche statisch oder automatisch erfolgen kann.



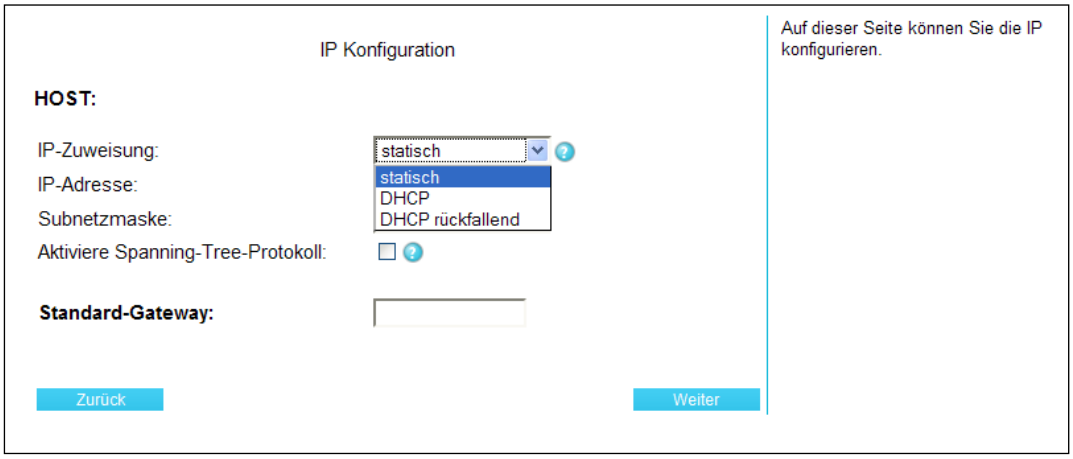
Statisch:

Wenn diese Option gewählt ist kann eine fest zugewiesene IP-Adresse eingetragen werden. Die statische IP-Zuweisung erfordert die Eingabe der IP-Adresse und der Subnetzmaske.

Die Default Werte sind:

IP-Adresse: **192.168.0.254**

Subnetzmaske: **255.255.255.0**



DHCP:

Die DHCP Funktion fordert eine IP-Adresse von einem DHCP-Server an und nimmt die Zuweisungen automatisch vor.

DHCP rückfallend:

Die Option ermöglicht die automatische Zuweisung der IP-Adresse. Sollte ein Fehler bei der automatischen Zuweisung auftreten, wechselt die IP-Zuweisung automatisch auf die statische Einstellung.

Aktiviere Spanning Tree Protokoll:

Das Spanning Tree Protokoll dient zur Vermeidung von Kreisläufen (Schleifen), speziell in geswitchten Netzwerkumgebungen.

Bei aktivierter Funktion ist es möglich redundante Netzwerkleitungen zu erzeugen.

Standard-Gateway:

Die IP-Adresse des Standard-Gateways dient dem Gerät dazu eine IP-Konfiguration zu einer Adresse außerhalb seines eigenen IP-Subnetzes aufzubauen (im Beispiel außerhalb 192.168.0.254). Die IP-Adresse selbst muss jedoch innerhalb dieses Netz-Bereiches liegen. Der Wert wird evtl. durch einen dynamischen DHCP Wert überschrieben, falls unter IP-Zuweisung DHCP konfiguriert wurde und der DHCP Server diese Option Unterstützt. Der Standard-Gateway kann nötig sein um z.B. einen NTP Zeitserver zu erreichen oder um die IP-Adresse wiederum selbst bei einer DHCP Server Einstellung an WLAN-Clients weiterzugeben.

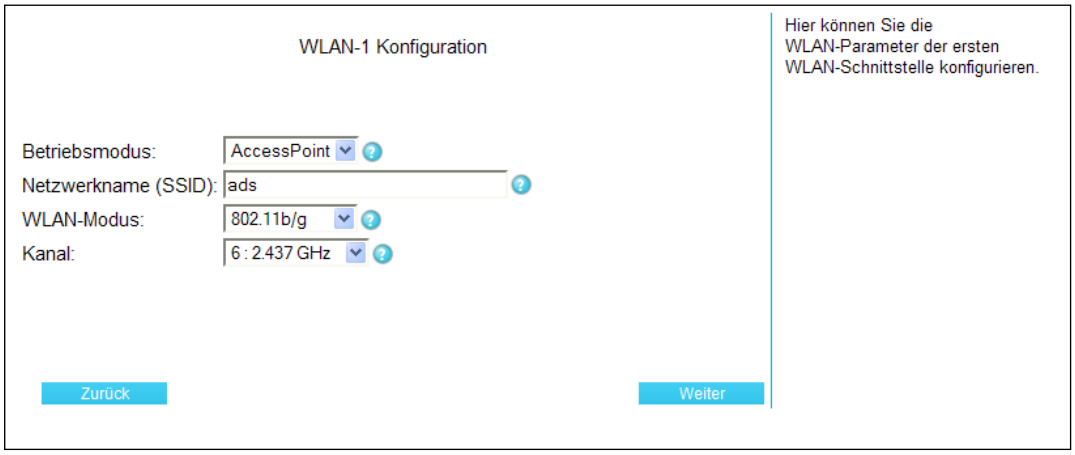
Es folgt ein Klick auf **Weiter**

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

7.1.2 WLAN-1 KONFIGURATION

Im nun folgenden Dialogfenster werden die relevanten Basis-Einstellungen für den WLAN-Betrieb konfiguriert.

ACCESS POINT-MODE:



BETRIEBSMODUS:

Hier erfolgt die Umschaltung zwischen den beiden Betriebsmodi **Access Point** oder **Access Client**.

Hinweis:

Der RAC (Access Client) hat an dieser Stelle keine Auswahlmöglichkeit. Er steht immer auf der Einstellung Access Client.

Access Point:

Im Modus Access Point bildet das Gerät einen Zugangspunkt zum Netzwerk für andere drahtlose Geräte (Clients).

Access Client:

Im Modus Client sucht der Access Client die Verbindung zu einem Access Point, um Verbindung zum Netzwerk aufnehmen zu können.

NETZWERKNAME (SSID):

In diesem Punkt wird der Name des Netzwerks vergeben. Es wird empfohlen, keine Namen zu verwenden, die Rückschlüsse auf das Unternehmen, Abteilung, oder Art der übertragenen Daten zulassen. Alle Clients, die eine Verbindung mit diesem Access Point aufbauen wollen, müssen diesen Netzwerknamen kennen.

Die Default-Einstellung ist: **ads**

Hinweis:

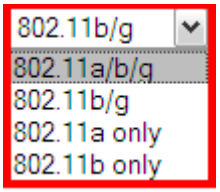
Die SSID kann maximal 32 Zeichen lang sein. Gültige Zeichen sind: a-z, A-Z, 0-9, Sonderzeichen: . _ - ? $ @ ! { } [ ] ( ) + # ; , < > | : * ~ % $ & / =

WLAN-MODUS:

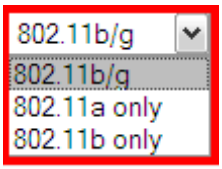
Hier kann der Funkstandard gewählt werden. Alle Clients, die mit dem Access Point kommunizieren sollen, müssen mit demselben Funkstandard ausgerüstet sein.

Die folgenden WLAN Modi können gewählt werden:

ACCESS CLIENT:



ACCESS POINT:

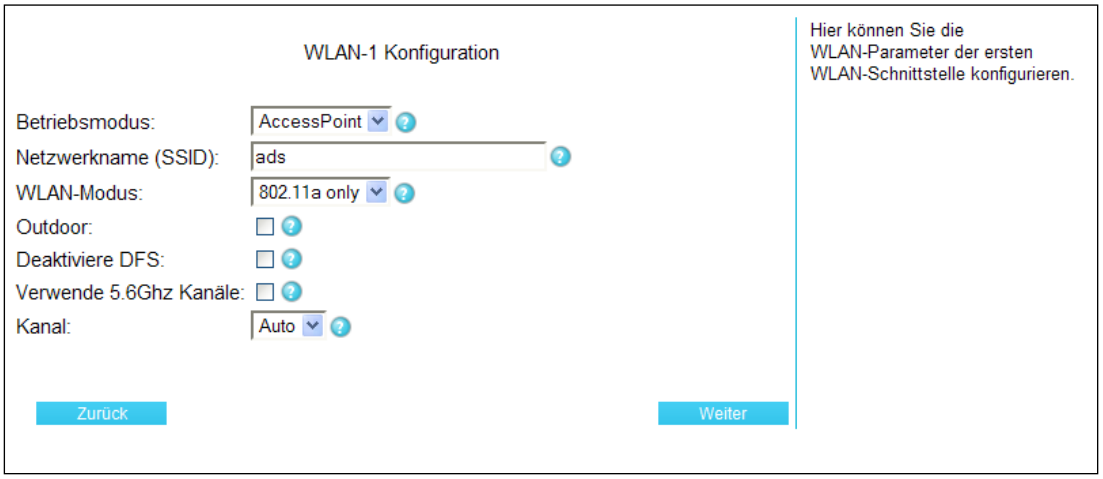


REGULIERUNGSBEHÖRDE

Hier muss das Land eingestellt werden, indem das Gerät betrieben wird. Durch diese Ländereinstellung wird sichergestellt, dass die verschiedenen nationalen Vorschriften der einzelnen Länder eingehalten werden.

WLAN1 (ACCESS POINT & ACCESS CLIENT) 5 GHZ – 802.11A (ETSI):

Wird der WLAN-Modus 802.11a (Access Point) oder 802.11a/b/g (Access Client) konfiguriert, dann ändern sich einige verfügbare Optionen:



Hinweis:

Die Option „Outdoor“ ist nur im Access Point Modus verfügbar. Die Option Deaktiviere DFS steht in beiden Modi zur Verfügung.

Indoor/Outdoor:

Muss aktiviert werden, falls der Access Point Teil einer Funkverbindung im Freien ist. Bestimmte Kanäle des 5GHz Bandes dürfen nicht im Freien verwendet werden, diese werden mit dieser Option ausgeschlossen. Bei Verwendung nur im Innenbereich kann die Option Indoor verwendet werden. Bei Access Clients spielt diese Option keine Rolle.

Deaktivere DFS:

Wird der Access Point NICHT im Freien betrieben darf DFS deaktiviert werden. Die Kanäle 36,40,44 und 48 dürfen dann auch von Hand fest eingestellt werden. Zusätzlich wird die maximal zulässige Abstrahlleistung reduziert. Im Client Betriebsmodus dagegen darf DFS auch im Freien deaktiviert werden.

Hinweis:

Im Client Modus ist die DFS Funktion Standardmäßig deaktivert. Durch die Radar-Erkennung während der Datenübertragung kann es insbesondere beim Client zu starken Interferenzen kommen welche dann als mögliche Radar Impulse ausgewertet müssen. Eine sehr hohe CPU Last und fehlerhafte häufige Radar-Detektionen sind die Folge. DFS sollte daher im Client Modus nur aktiviert werden wenn die höhere Abstrahlleistung des Client von 23dB überschritten wird und 30dBm nötig sind um eine stabile Datenverbindung zu erreichen. Befindet sich in unmittelbarer Nähe ein weiteres 5 GHz Gerät kann dies ebenfalls zu erheblichen Störungen des Client-Modus führen wenn DFS aktiv ist.

Achtung:

Falsche Einstellungen für den Betriebsort können zu illegalen Funkeinstellungen führen, die durch Behörden geahndet werden.

Der Betreiber des Gerätes trägt die Verantwortung für die richtige Einstellung

Verwende 5.6Ghz Kanäle:

Es werden die Kanäle 120,124 und 128 aktiviert. Bei aktivierter DFS-Funktion muss eine Ansprechzeit (Channel Availability Check Time) von 10 Minuten eingehalten werden.

KANAL:

Das Gerät kann nach Wunsch den Sendekanal automatisch wählen oder auch manuell eingestellt werden. Es wird empfohlen, die automatische Kanalwahl (**Auto**) zu aktivieren. Nur dann kann das Gerät bei Störungen auf diesem Kanal selbständig auf einen anderen, störungsfreien Kanal umschalten.

Hinweis:

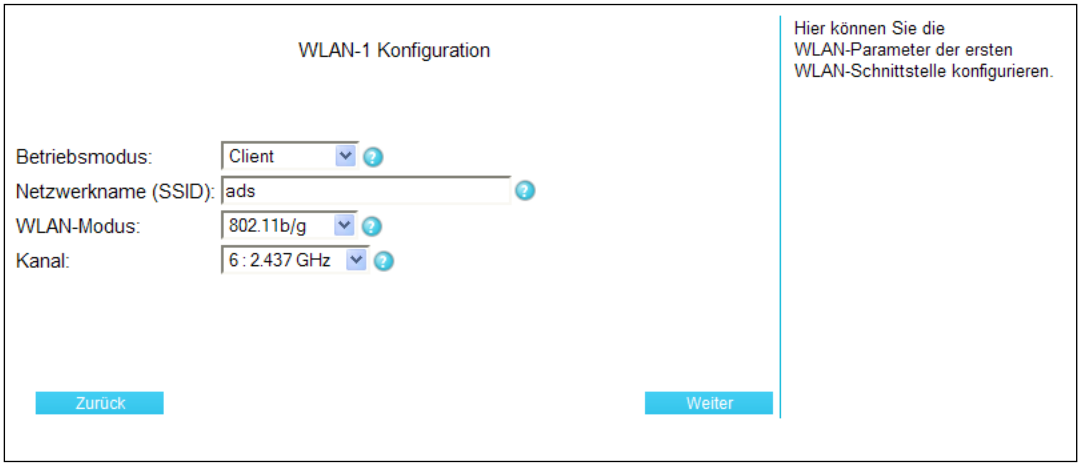
5GHz Kanäle lassen sich nicht fest konfigurieren, stattdessen werden Sie zufällig unter den freien Kanälen gewählt (Diese Eigenschaft ist vom Gesetzgeber für Sendezulassung vorgeschrieben).

Werden andere WLANs parallel betrieben, ist eine manuelle Funkfeldplanung zur Vermeidung von Einschränkungen in der Funkkommunikation notwendig. In diesem Fall sollte der Sendekanal manuell vergeben werden.

Beachten Sie das DFS ausgeschaltet sein muss um die Kanäle manuell auszuwählen.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

ACCESS CLIENT MODE:

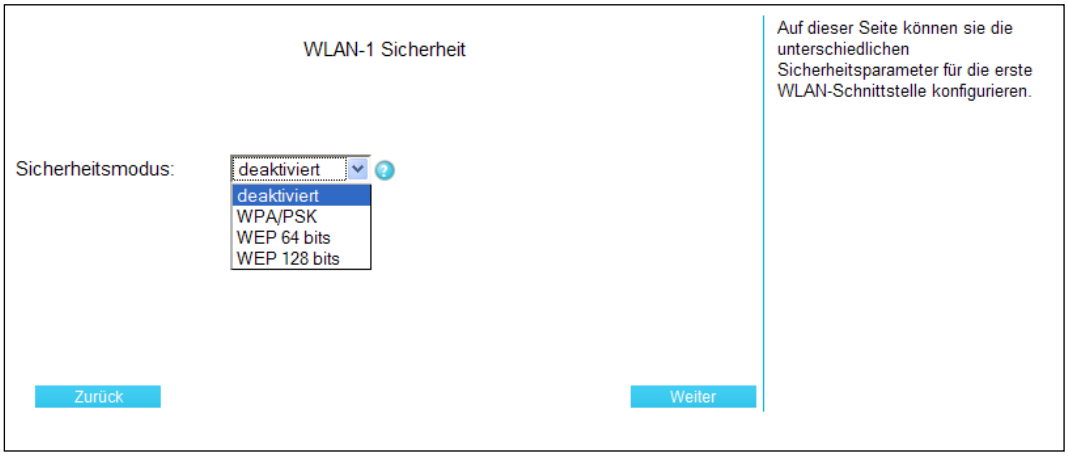


Der Client Mode unterscheidet sich in folgenden Einstellungen:

Deaktiviere DFS:
Bei aktivierter Funktion wird DFS auf dem 5GHz Band deaktiviert. Die Kanäle die ohne DFS verwendet werden können, sind dann manuell anwählbar. Diese Option darf nicht aktiviert werden wenn das Gerät im Freien verwendet wird.

WLAN 1 SICHERHEIT

Die WLAN Sicherheit ermöglicht die Konfiguration des entsprechenden Sicherheitsstandards für das WLAN-Netzwerk. Zur Auswahl stehen folgende Modi:

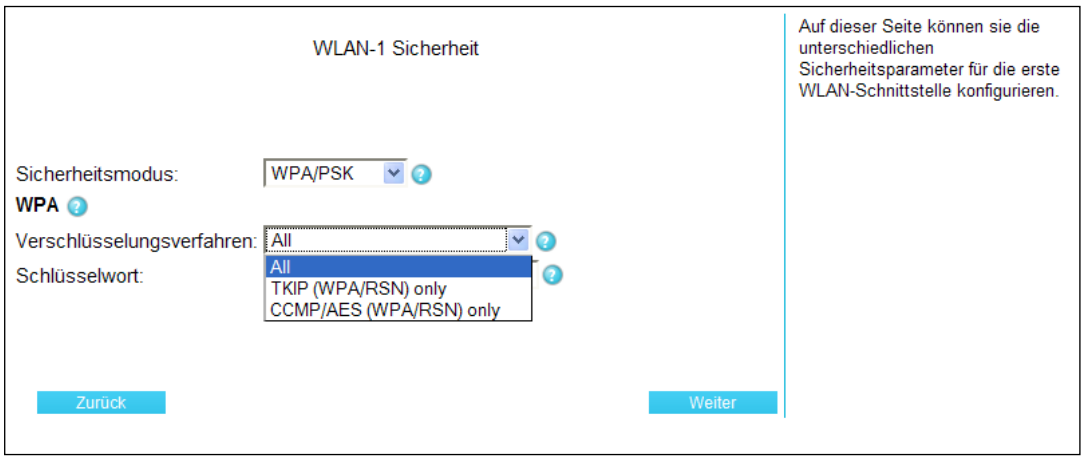


WPA/PSK

Im WPA/PSK Modus wird ein Schlüsselwort in Kombination mit einem speziellen Verschlüsselungsverfahren verwendet. Das Schlüsselwort (Pre shared key) darf minimal 8 und maximal 63 Zeichen enthalten. Es wird empfohlen keine Wörter sondern Kombinationen aus Buchstaben, Zahlen zu verwenden, um die Sicherheit optimal zu gewährleisten.

Hinweis:

8-63 Zeichen, Gültige Zeichen sind alle ASCII Zeichen von 32-116



Verschlüsselungsverfahren:

Es besteht die Möglichkeit alle Verschlüsselungsverfahren oder ein spezielles Verschlüsselungsverfahren zu verwenden. Hierbei ist zu beachten, dass der Standard WPA 2 von allen Geräten unterstützt werden muss, um eine Funktionalität zu gewährleisten.

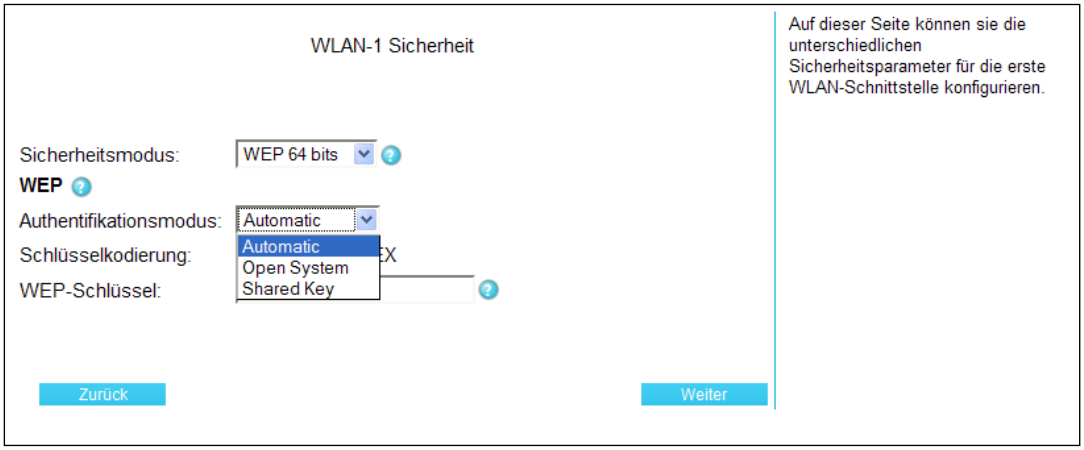
WEP 64 BITS / WEP 128 BITS

Im WEP 64 Bits / 128 Bits Modus wird wie bei WPA ein Schlüsselwort verwendet welches den Zugang zum WLAN-Netzwerk ermöglicht. Der Unterschied besteht darin, dass im WEP-Modus der Schlüssel nicht verändert wird, sondern statisch bleibt.

Hinweis:

Es wird empfohlen den Verschlüsselungstandard WPA zu verwenden, da eine WEP Verschlüsselung einen heutzutage unzureichenden Sicherheitsstandard darstellt.

Authentifikationsmodus:



Automatic:

Der Modus Automatic wählt den Authetifikationsmodus selbständig.

Open System:

Die **Open System** Authentication ist die Standard-Authentifizierung.

Shared Key:

Die Shared Key Authentication verwendet einen erweiterten Handshake Mechanismus beim Einbuchungsvorgang, der jedoch keine weitere Sicherheit bringt.

Schlüsselkodierung:

Wahlweise kann eine Schlüsselkodierung ASCII oder HEX verwendet werden. ASCII ist eine 7-Bit Kodierung, HEX verwendet eine 16-Bit Kodierung.

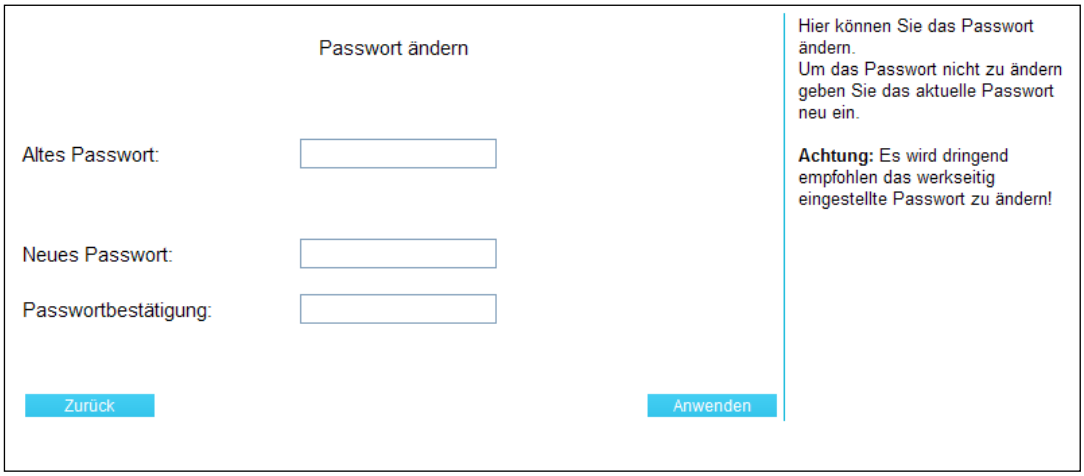
WEP-Schlüssel:

Der WEP-Schlüssel ist bei ASCII-Wahl auf 5 Zeichen begrenzt. HEX ermöglicht die Eingabe eines 10 stelligen WEP-Schlüssels. Bei der Wahl des Schlüssels sollten keine Wörter, sondern Buchstaben und Zahlenkombinationen verwendet werden.

Bestätigen Sie mit **Weiter**

7.1.3 PASSWORT ÄNDERN

Das Dialogfenster ermöglicht das Ändern des Passworts.


Passwort ändern
Hier können Sie das Passwort ändern.
Um das Passwort nicht zu ändern geben Sie das aktuelle Passwort neu ein.
Altes Passwort:
Achtung: Es wird dringend empfohlen das werkseitig eingestellte Passwort zu ändern!
Neues Passwort:
Passwortbestätigung:
Zurück
Anwenden

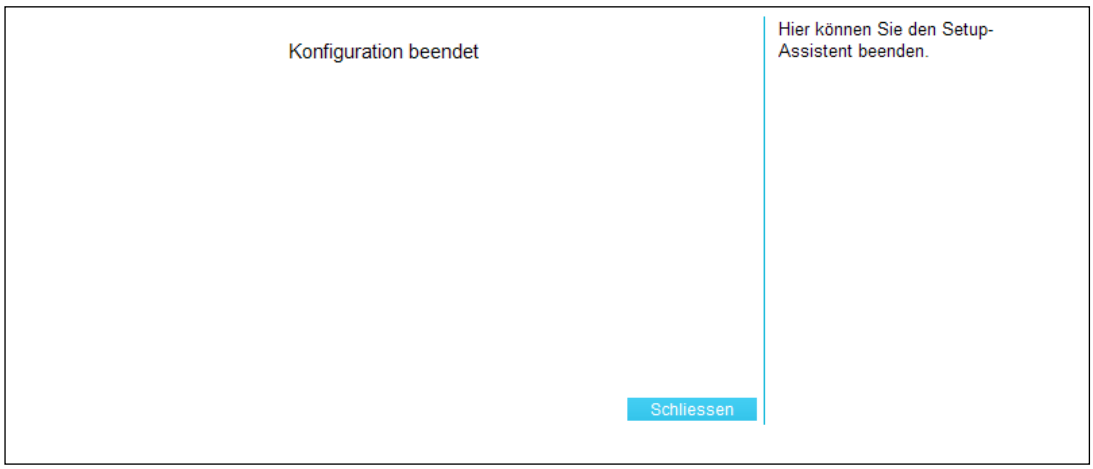
Um ein bereits vergebenes Passwort zu ändern, geben Sie das aktuelle Passwort in das Feld Altes Passwort ein.

Wählen Sie ein neues Passwort und bestätigen Sie dieses in den nächsten beiden Feldern. Sollten Sie kein Passwort vergeben haben lassen Sie die Felder leer.

Klicken Sie im Anschluss auf **Anwenden.**

Ihre Einstellungen werden gespeichert…

Der Setup Assistent ist nun abgeschlossen.


Konfiguration beendet
Hier können Sie den Setup-Assistent beenden.
Schliessen

7.2 KONFIGURATION MIT HILFE DES PAKETFILTERES

Ein Paketfilter ist im Gerät dafür zuständig, Datenpakete in erwünschten und nicht erwünschten Datenverkehr zu klassifizieren und entsprechende Aktionen einzuleiten.

Über den Pfad **Konfiguration > Paketfilter** kann der Paketfilter gestartet werden, wenn er nicht direkt im Anschluss des **Setup-Assistenten** gestartet wurde.

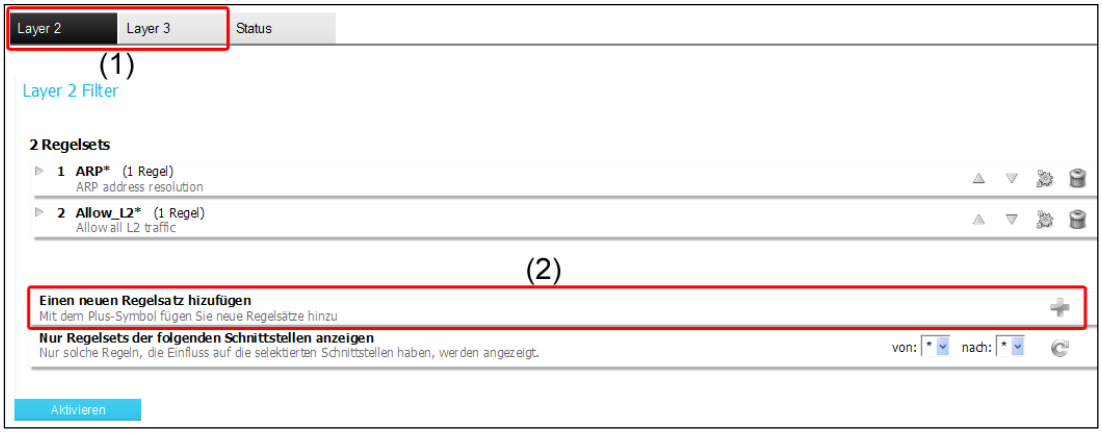
Die Startseite des Paketfilters ermöglicht das Hinzufügen von neuen Regelsets und das Bearbeiten von bestehenden Regelsets.

Hinweis:

Eine Regel beschreibt die Konfiguration einer spezifischen Filteranweisung.
Ein Regelset kann aus bis zu zehn separaten Regeln bestehen.

7.2.1 HINZUFÜGEN EINER REGEL

Das Hinzufügen eines Regelsets erfordert zunächst die Auswahl des Layers über die jeweiligen **Reiter**(**1**). Im Transparent Bridge Modus ist in den meisten Fällen eine Filterung auf überbrückten Ethernet Schnittstellen (Layer 2) nötig, während im IP Router Modus oder bei Verwendung des SERVICE Modems auch eine Auswahl von eigenständigen IP-Schnittstellen (Layer 3) in Frage kommt.



Überbrückte Ethernet Schnittstellen (Layer 2):

Entspricht der Ethernet Filterungsebene. Diese Einstellung ermöglicht z.B. die Filterung anhand von Ethernet MAC-Adressen oder Netzwerk-Protokollen, die keine IP-Adressen verwenden. Es ist jedoch auch eine Filterung auf Basis von IP-Protokoll Merkmalen möglich.

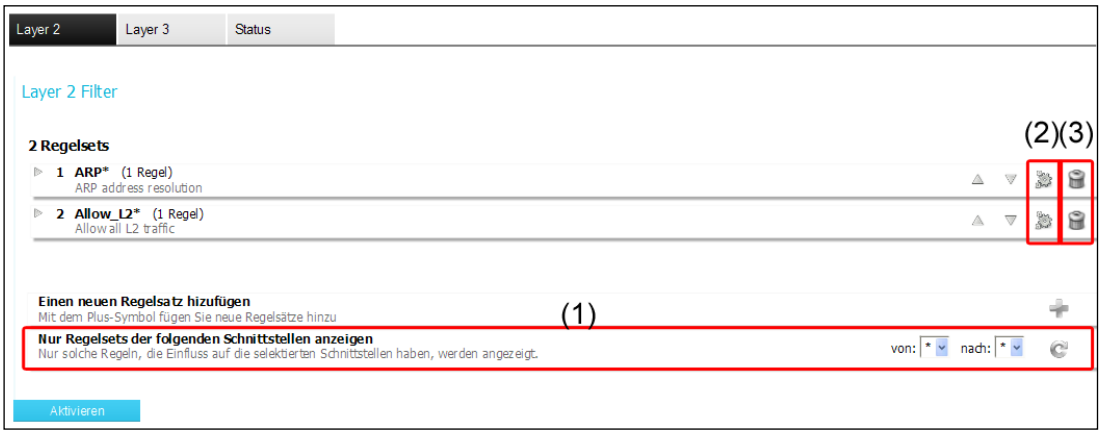
Eigenständige IP-Schnittstellen (Layer 3):

Auf dieser Ebene ist das Filtern ausschließlich auf Basis von IP-Protokoll Merkmalen möglich, da zwischen Schnittstellen der Ebene 3 ausschließlich IP-Datenverkehr stattfindet.

Über den Button **Einen neuen Regelsatz hinzufügen** (**2**) kann eine neue oder vorkonfigurierte Regel für das ausgewählte Layer erstellt oder hinzugefügt werden. Eine Beschreibung des Erstellens eines neuen Regelsets finden sie unter den Kapiteln **Neues Regelset auf Layer 2 definieren** und **Neues Regelset auf Layer 3 definieren**. Im Kapitel **Laden eines vorkonfigurierten Regelsets** werden die vordefinierten Regelsets beschrieben.

7.2.2 Ändern und Suchen von bestehenden Regelsets

Sollten Sie bereits Regeln erstellt oder geladen haben, erscheinen diese in der Regelübersicht. Wenn Sie eine Regel suchen, können Sie über die Drop-Down-Felder **Von**, **Nach** (**1**) die Filterkriterien für die gesuchten Regelsets einschränken.



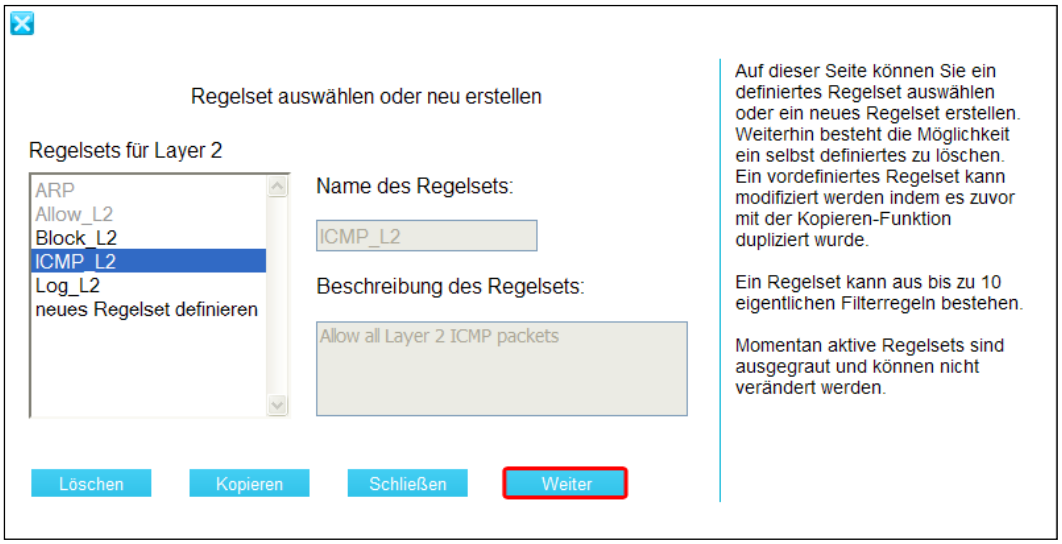
Der Button **Bearbeiten** (**2**) ermöglicht das nachträgliche Ändern des ausgewählten Regelsets. Über **Löschen** (**3**) wird das ausgewählte Regelset entfernt.

Hinweis:

Über die Pfeile vor jedem Regelset können detailliertere Informationen zum ausgewählten Regelset angezeigt werden.

7.2.3 Laden einer vorkonfigurierten Regel

Wählen Sie ein vorkonfiguriertes Regelset aus.
Das Dialogfenster zeigt die vorkonfigurierten Regelsets auf der linken Seite.


Regelset auswählen oder neu erstellen
Regelsets für Layer 2
ARP
Allow_L2
Block_L2
ICMP_L2
Log_L2
neues Regelset definieren
Name des Regelsets:
ICMP_L2
Beschreibung des Regelsets:
Allow all Layer 2 ICMP packets
Auf dieser Seite können Sie ein definiertes Regelset auswählen oder ein neues Regelset erstellen. Weiterhin besteht die Möglichkeit ein selbst definiertes zu löschen. Ein vordefiniertes Regelset kann modifiziert werden indem es zuvor mit der Kopieren-Funktion dupliziert wurde.
Ein Regelset kann aus bis zu 10 eigentlichen Filterregeln bestehen.
Momentan aktive Regelsets sind ausgegraut und können nicht verändert werden.
Löschen
Kopieren
Schließen
Weiter

Beispielhaft sind folgende Default-Regelsets in den Layerebenen 2 & 3 vorkonfiguriert.

Regelsets für Layer 2

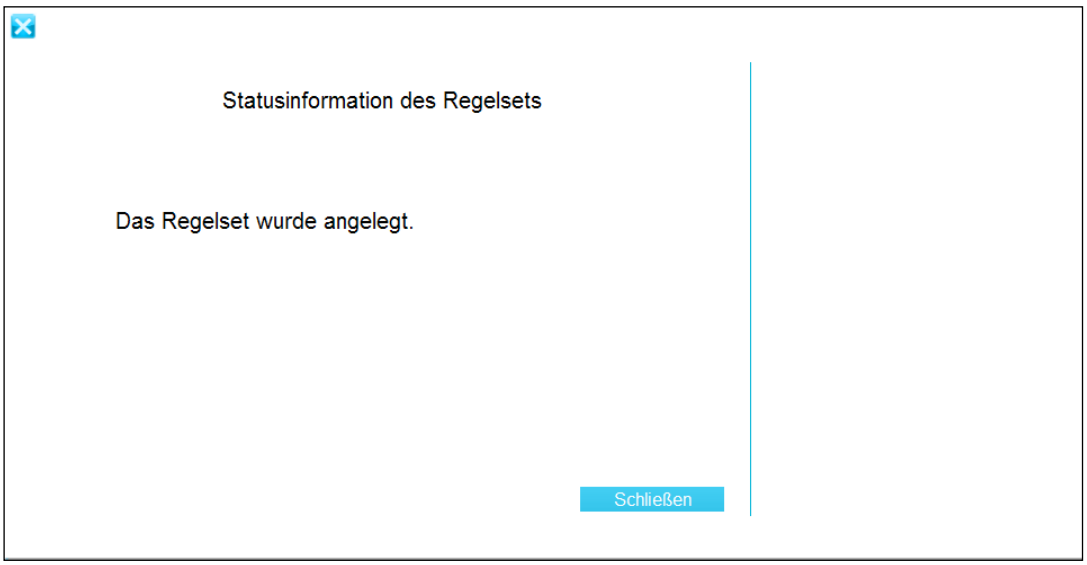
Name	Kurze Erläuterung
ARP	Adress Resolution Protocol ermöglicht die Zuordnung von Netzwerk auf- Hardwareadressen
Allow_L2	Erlaubt den gesamten Datenverkehr auf Layer 2
Block_L2	Verwirft alle Datenpakete (blockiert den gesamten Datenverkehr) auf Layer 2
ICMP_L2	Erlaubt den gesamten Datenverkehr über ICMP auf Layer 2
Log_L2	Protokolliert im Eventlog und verwirft alle Datenpakete auf Layer 2

Wählen Sie das zu ladende Regelset und bestätigen Sie mit **Weiter.**

Regelsets für Layer 3

Name	Kurze Erläuterung
ALLOW_L3	Erlaubt den gesamten Datenverkehr auf Layer 3
BLOCK_L3	Verwirft alle Datenpakete (blockiert den gesamten Datenverkehr) auf Layer 3
ICMP_L3	Erlaubt den gesamten Datenverkehr über ICMP auf Layer 3
Log_L3	Protokolliert im Eventlog und verwirft alle Datenpakete auf Layer 3

Bestätigen Sie die angezeigte Meldung mit **Schließen**



Nach erfolgreicher Aktivierung ist das Regelset in der Filterübersicht zu sehen.

7.2.4 NEUES REGELSET AUF LAYER 2 DEFINIEREN

Hinweis:
Wenn Sie nach Filterebene Layer 3 konfigurieren möchten, fahren Sie mit dem Abschnitt „**Neues Regelset auf Layer 3 definieren**“ fort.

Wählen Sie den Menüpunkt **Neues Regelset definieren**

Regelset auswählen oder neu erstellen
Regelsets für Layer 2
ARP
Allow_L2
Block_L2
ICMP_L2
Log_L2
neues Regelset definieren
Name des Regelsets:
Testregel
Beschreibung des Regelsets:
Testregel
Löschen
Kopieren
Schließen
Weiter
Auf dieser Seite können Sie ein definiertes Regelset auswählen oder ein neues Regelset erstellen. Weiterhin besteht die Möglichkeit ein selbst definiertes zu löschen. Ein vordefiniertes Regelset kann modifiziert werden indem es zuvor mit der Kopieren-Funktion dupliziert wurde.
Ein Regelset kann aus bis zu 10 eigentlichen Filterregeln bestehen.
Momentan aktive Regelsets sind ausgegraut und können nicht verändert werden.

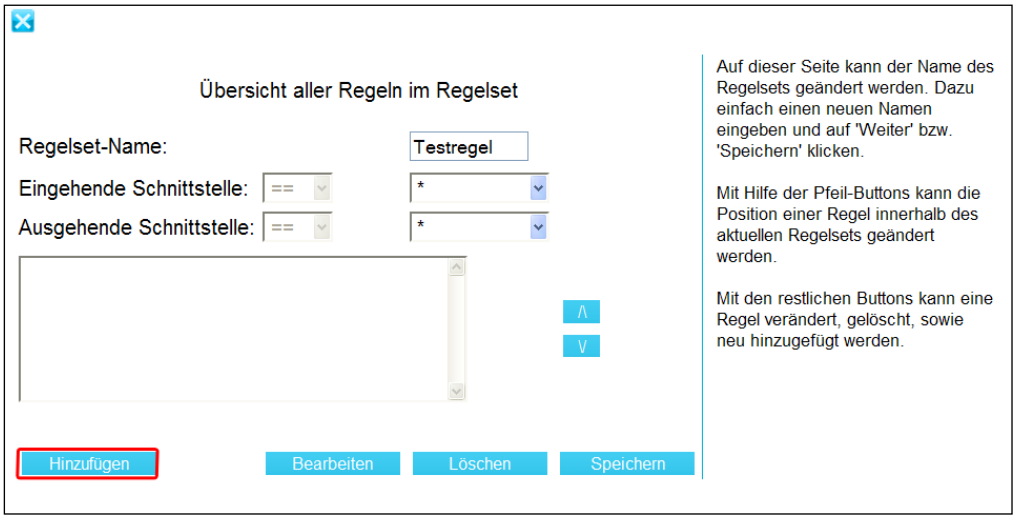
Vergeben Sie einen Namen und eine Beschreibung für ihr Regelset.

Hinweis:
Der Name des Regelsets ist auf 16 Zeichen beschränkt. Unlaute können nicht verwendet werden.

Bestätigen Sie ihre Eingabe mit **Weiter**

Layer und Schnittstellen des Regelsets

Über das Dialogfenster wird die Laufbahn der Pakete eingestellt, auf die dieses Regelset angewendet werden soll. Es werden die eingehende Schnittstelle (auf der die Pakete hereinkommen) sowie die ausgehende Schnittstelle (auf der die Pakete das Gerät nach Akzeptanz verlassen soll) benötigt.


Übersicht aller Regeln im Regelset
Regelset-Name:
Testregel
Eingehende Schnittstelle:
==
*
Ausgehende Schnittstelle:
==
*
Hinzufügen
Bearbeiten
Löschen
Speichern
Auf dieser Seite kann der Name des Regelsets geändert werden. Dazu einfach einen neuen Namen eingeben und auf 'Weiter' bzw. 'Speichern' klicken.
Mit Hilfe der Pfeil-Buttons kann die Position einer Regel innerhalb des aktuellen Regelsets geändert werden.
Mit den restlichen Buttons kann eine Regel verändert, gelöscht, sowie neu hinzugefügt werden.

Symbolerläuterung	
==	Ausgewählte Schnittstelle wird verwendet
!=	Alle Schnittstellen, **außer** der Ausgewählten werden verwendet

Beispiel:

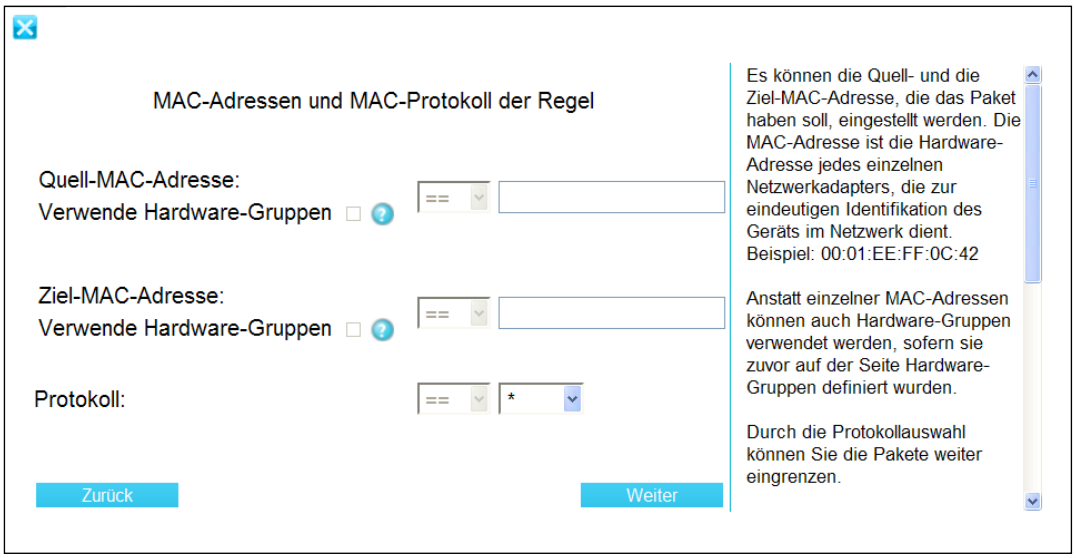
Schnittstelle	Auswahl	Folge
Eingehende Schnittstelle :**HOST**	==	filtert alle eingehenden Datenpakete auf HOST
Ausgehende Schnittstelle: **WLAN-1**	!=	filtert alle ausgehenden Datenpakete auf allen Ports, **außer WLAN-1**

Bestätigen Sie ihre Eingabe mit **Hinzufügen**

MAC-Adressen und MAC-Protokoll der Regel

Im nun erscheinenden Dialogfenster lassen sich die MAC-Adressen der jeweiligen Eingänge bzw. Ausgänge definieren.

Die **Quell- MAC Adresse** definiert den Port auf welchem Daten gesendet werden. Die **Ziel MAC- Adresse** definiert den Port auf dem Daten empfangen werden.


MAC-Adressen und MAC-Protokoll der Regel
Quell-MAC-Adresse:
Verwende Hardware-Gruppen
Ziel-MAC-Adresse:
Verwende Hardware-Gruppen
Protokoll:
==
*
Zurück
Weiter
Es können die Quell- und die Ziel-MAC-Adresse, die das Paket haben soll, eingestellt werden. Die MAC-Adresse ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Beispiel: 00:01:EE:FF:0C:42
Anstatt einzelner MAC-Adressen können auch Hardware-Gruppen verwendet werden, sofern sie zuvor auf der Seite Hardware-Gruppen definiert wurden.
Durch die Protokollauswahl können Sie die Pakete weiter eingrenzen.

Wenn Sie eine feste Verbindung zwischen 2 Geräten verwenden, können Sie die MAC-Adressen der jeweils verfügbaren Geräte hier fest definieren. Ansonsten belassen Sie die Felder mit dem Sternsymbol.

Hinweis:

Wenn die Option “Verwende Hardware-Gruppen“ aktiviert ist, können die hinzugefügten Hardware-Gruppen ausgewählt werden. Verwenden Sie diese Option wenn Sie Regeln für mehr als eine MAC-Adresse zuweisen möchten.

Hinweis:

Wenn Sie eine dauerhafte Verbindung zwischen zwei fest definierten Geräten verwenden möchten, können Sie die MAC-Adressen der jeweiligen Geräte hier festlegen.

Protokoll	Beschreibung
ARP	Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, das die Zuordnung von Netzwerkadressen zu Hardwareadressen möglich macht. Obwohl es nicht auf Ethernet- und IP-Protokolle beschränkt ist, wird es fast ausschließlich im Zusammenhang mit IP-Adressierung auf Ethernet-Netzen verwendet.
IPV4	IPv4 (Internet Protocol Version 4), früher einfach IP, ist die vierte Version des Internet Protocols (IP). Es war die erste Version des Internet Protocols, welche weltweit verbreitet und eingesetzt wurde und bildet eine wichtige technische Grundlage des Internets.
Vlan	Ein Virtual Local Area Network (VLAN) ist ein virtuelles lokales Netz innerhalb eines physischen Netzes. Eine weit verbreitete technische Realisierung von VLANs ist teilweise im Standard IEEE 802.1Q definiert.

Other	Ermöglicht die Auswahl eines anderen Protokolls.

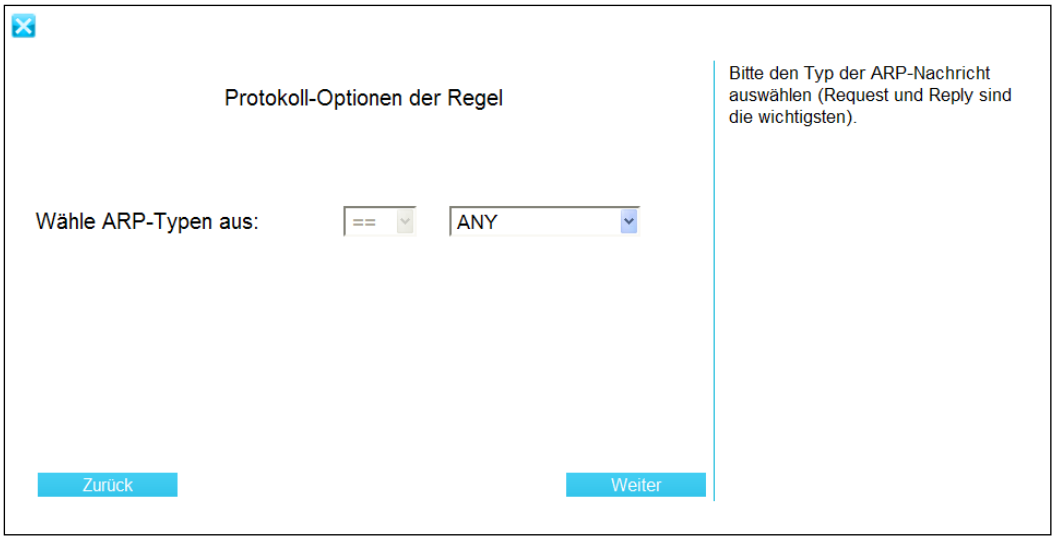
Hinweis:
Wenn Sie kein spezielles Protokoll wünschen, wählen Sie das Standard-Feld mit dem Sternsymbol. Sobald ein spezielles Protokoll ausgewählt wird, können neue Einstellungen protokollspezifisch getätigt werden.

PROTOKOLLOPTIONEN

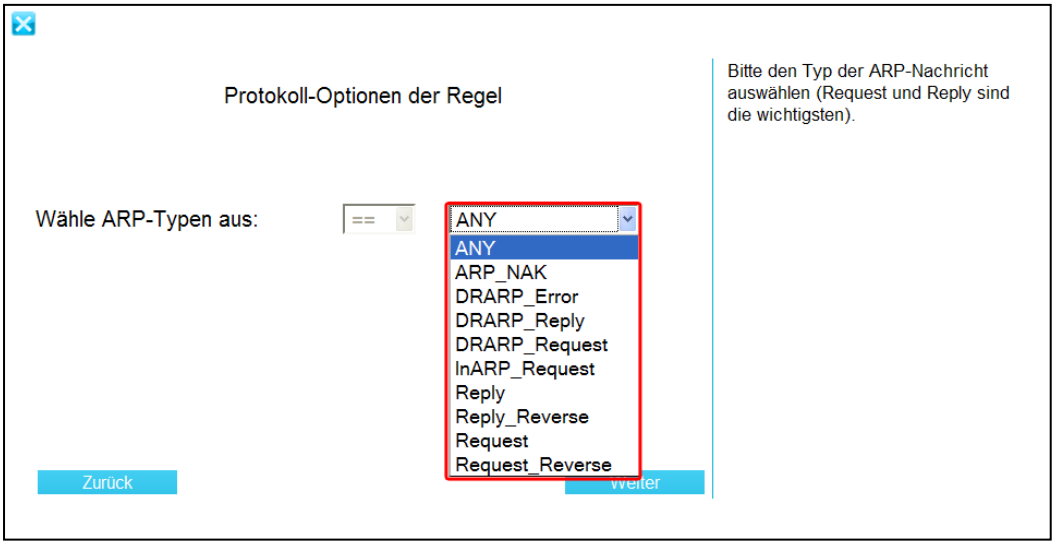
Folgende Konfigurationsmöglichkeiten bestehen, wenn Sie eines der Protokolle ARP, IPV4, VLAN oder Other gewählt haben:

Folgende Konfigurationsmöglichkeiten bestehen bei einer speziellen Protokoll-Auswahl. Wenn Sie kein spezielles Protokoll gewählt haben, bestätigen Sie mit **Weiter** und können mit Kapitel **Verhalten und Name der Regel** fortfahren.

ARP:

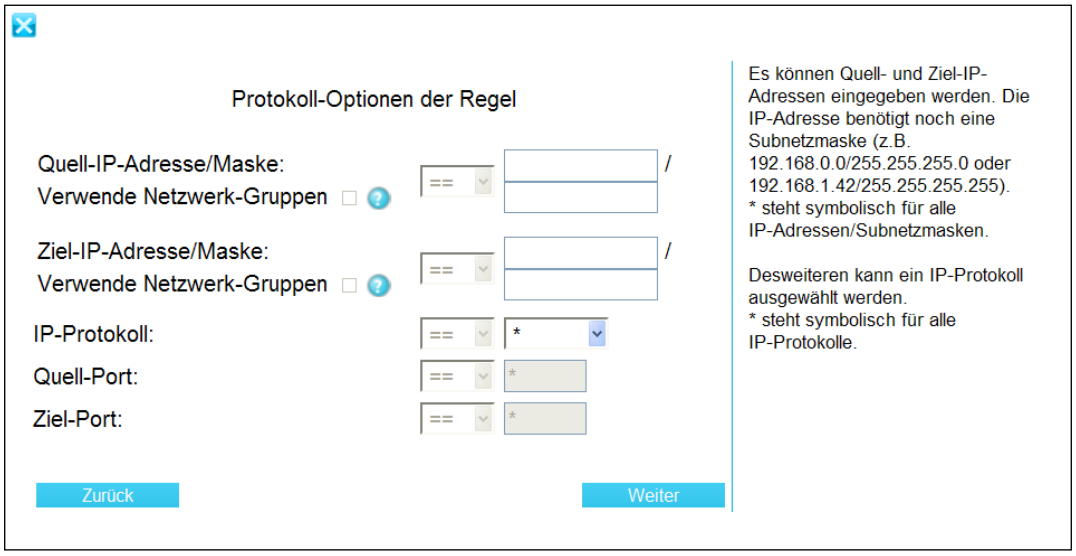


Das Protokoll ARP erlaubt folgende Auswahlmöglichkeiten:



IPV4:

Das IPV4 Protokoll erfordert die Eingabe der Quell- und Ziel-IP-Adresse. Zusätzlich muss noch jeweils eine Subnetzmaske für Quell-und Ziel-IP-Adresse angegeben werden.

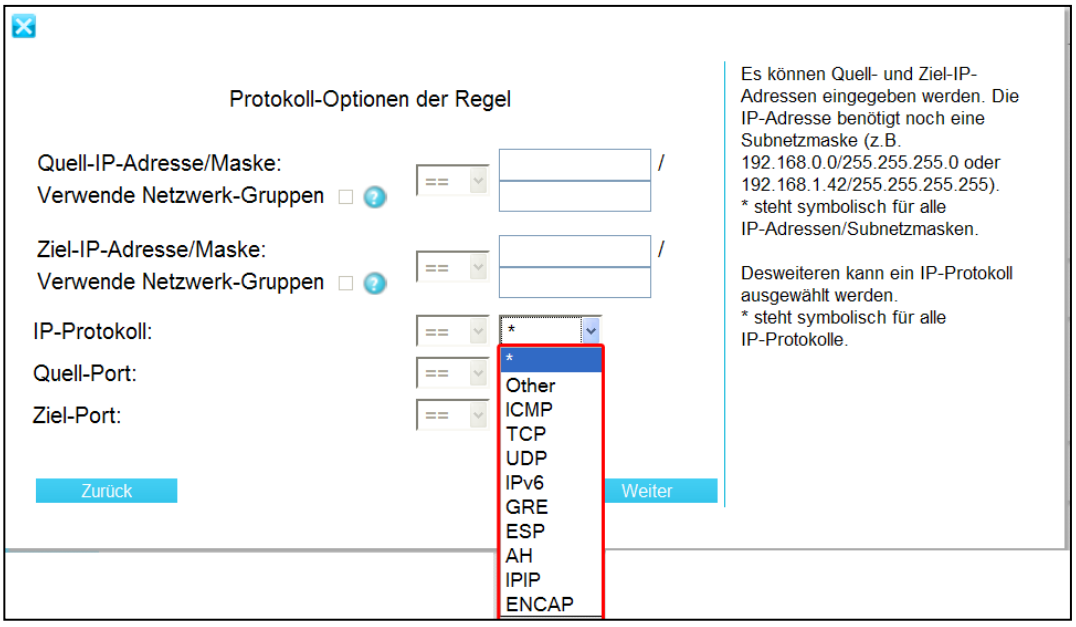


Das IPV4 Protokoll ermöglicht eine weitere umfangreiche Auswahl an Filterkriterien. Es kann auf Quell-IP-Adresse, Ziel-IP-Adresse, IP-Protokoll, Quell- und Ziel-Port gefiltert werden.

Hinweis:

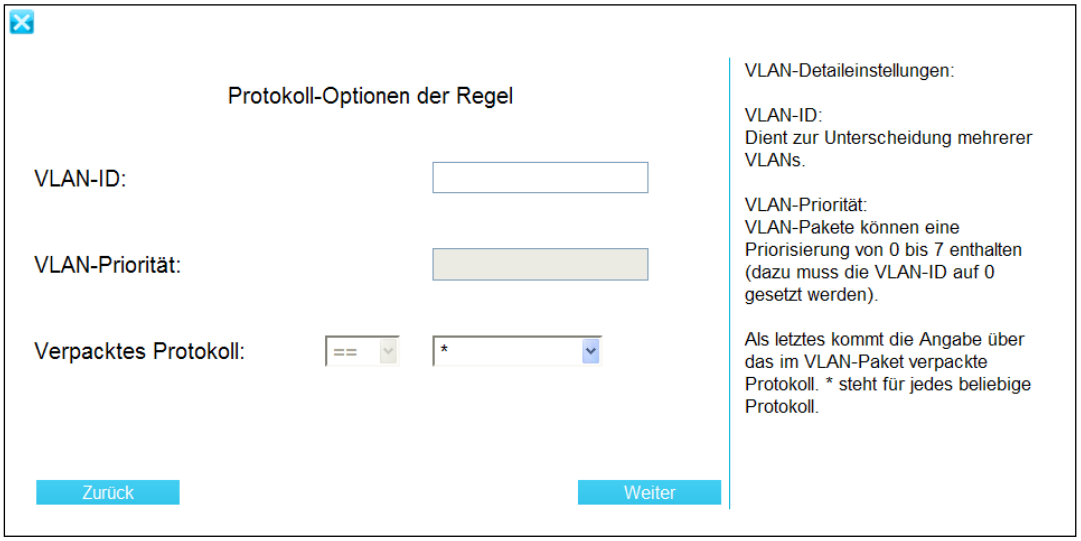
TCP/UDP Ports lassen sich als Port-Ranges angeben. Z.B. 80:88 für 80-88, :1024 (alle Ports<1024), oder 1024: (alle Ports größer 1024)

Unter IP-Protokolle stehen folgende Protokolle zur Auswahl:



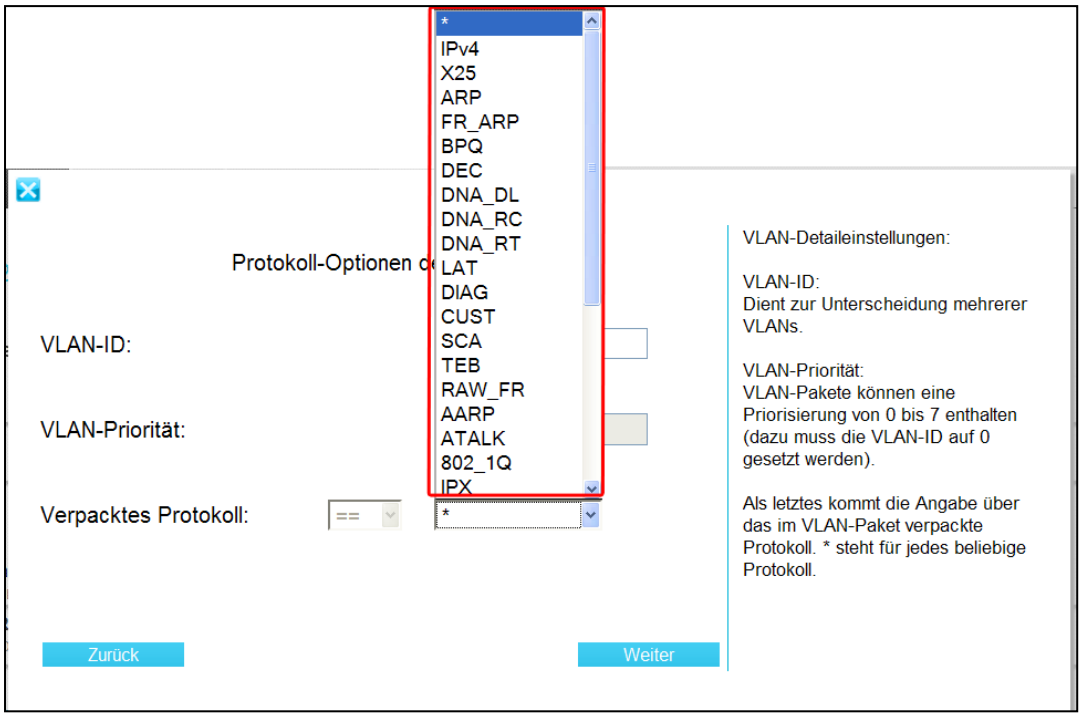
VLAN:

Das VLAN Protokoll erfordert die Angabe der VLAN-ID, der VLAN-Priorität und die Angabe des verpackten Protokolls.



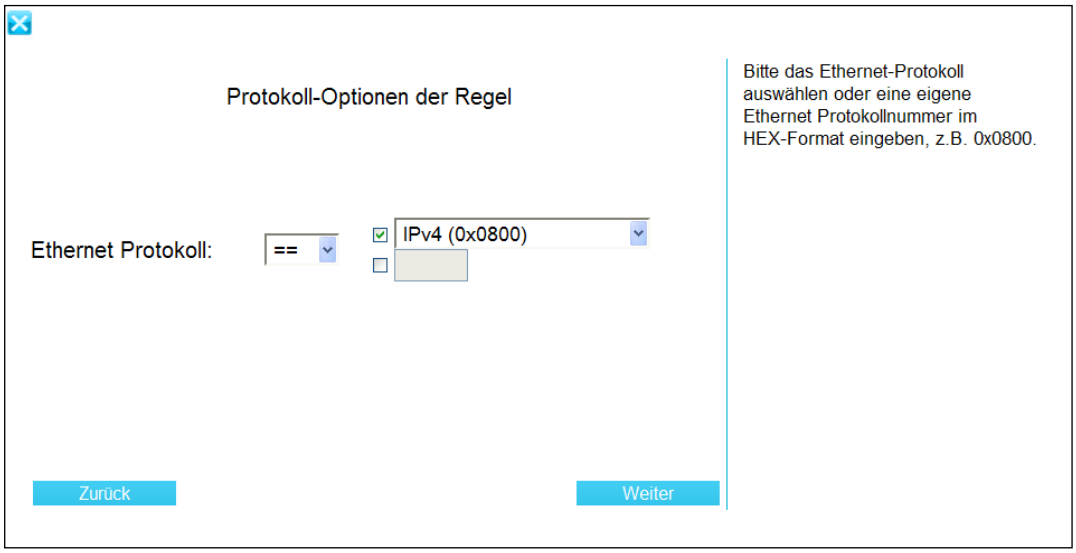
Das VLAN Protokoll erfordert die Angabe der VLAN-ID, der VLAN-Priorität und die Angabe des verpackten Protokolls.

Das verpackte Protokoll enthält eine hohe Anzahl an verschiedenen Protokollvarianten zur Auswahl. Sie können auswählen, ob Sie ein spezifisches Protokoll oder alle außer diesem spezifischen Protokoll verwenden möchten.

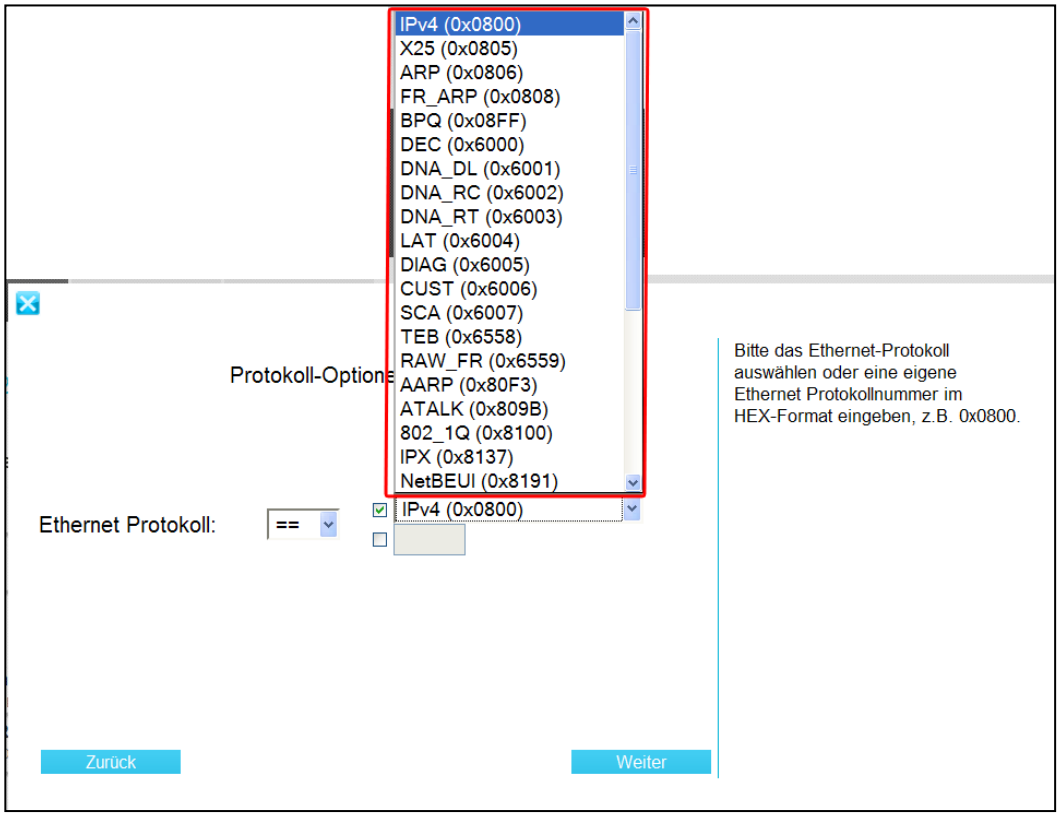


OTHER:

Mit Other wird das Layer 3 Protokoll gewählt.

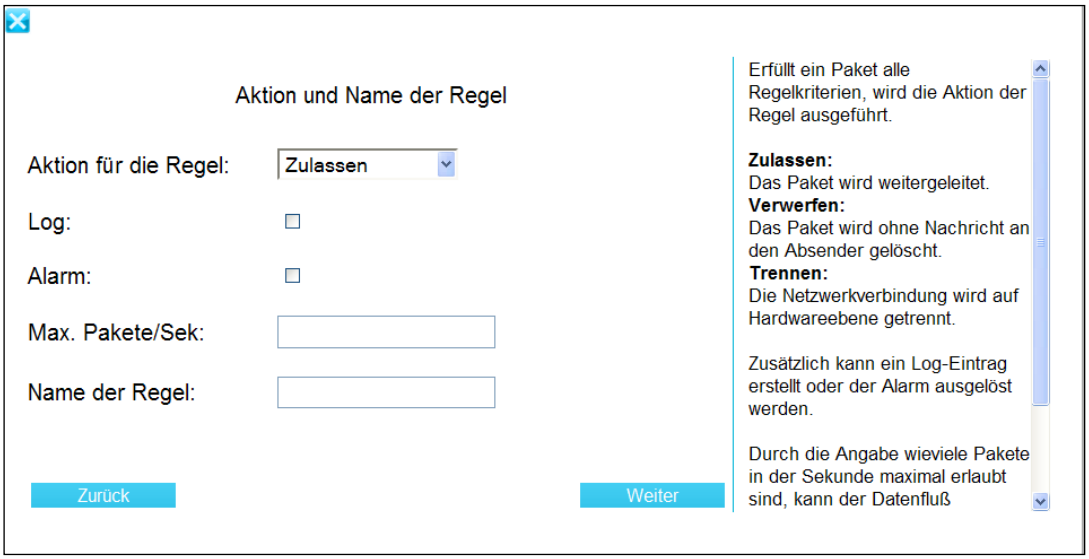


Other enthält eine hohe Anzahl an verschiedenen Protokollen zur Auswahl. Sie können auswählen, ob Sie ein spezifisches Protokoll oder alle außer diesem spezifischen Protokoll verwenden möchten.



AKTION UND NAME DER REGEL:

Das nächste Feld ermöglicht das Verhalten der Regel genauer zu definieren. Unter dem Menüpunkt **Aktion für die Regel** können Sie festlegen wie das Gerät mit einem Paket verfahren soll.


Aktion und Name der Regel
Aktion für die Regel:
Zulassen
Log:
Alarm:
Max. Pakete/Sek:
Name der Regel:
Zurück
Weiter
Erfüllt ein Paket alle Regelkriterien, wird die Aktion der Regel ausgeführt.
Zulassen:
Das Paket wird weitergeleitet.
Verwerfen:
Das Paket wird ohne Nachricht an den Absender gelöscht.
Trennen:
Die Netzwerkverbindung wird auf Hardwareebene getrennt.
Zusätzlich kann ein Log-Eintrag erstellt oder der Alarm ausgelöst werden.
Durch die Angabe wieviele Pakete in der Sekunde maximal erlaubt sind, kann der Datenfluß

Aktion für die Regel:
Zur Auswahl stehen:

Zulassen:	Das Paket wird weitergeleitet.
Verwerfen:	Das Paket wird ohne Nachricht an den Absender gelöscht.

Log:
Es wird ein Log-Eintrag erstellt und somit protokolliert.

Alarm:
Es wird der Alarmausgang gesetzt.

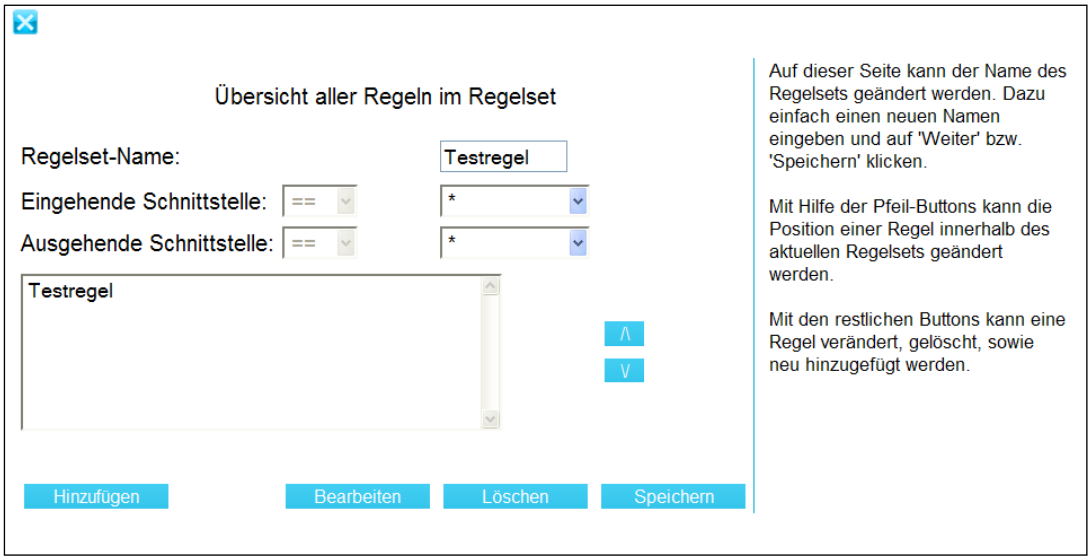
Max.Pakete/Sek:
Hier kann die maximale Paketrate pro Sekunde festgelegt werden, die als Obergrenze gegen einen Denial-of-Service eingestellt werden kann. Dies ist ebenfalls sinnvoll, um Regeln die in einem häufigen Intervall einen Eventlogeintrag erzeugen würden, zu begrenzen.

Name der Regel:
Definieren Sie einen eindeutigen Regelnamen. Es ist zwingend notwendig, dass Sie einen Namen für die Regel des Regelsets vergeben.

Bestätigen Sie mit: **Weiter**

ÜBERSICHT ALLER REGELN:

Das Dialogfenster zeigt die einzelnen Regeln des Regelsets an, diese können in ihrer Reihenfolge geändert werden. Des Weiteren kann der Regelsetname geändert werden.



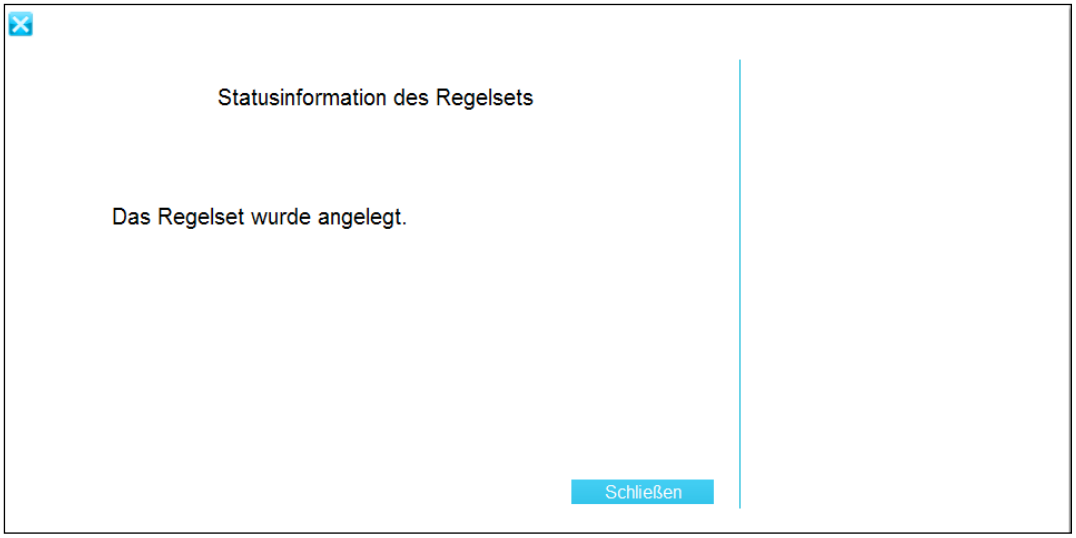
Über den Button **Hinzufügen** startet der Einrichtungsprozess erneut und eine neue Regel kann definiert werden. Der Button **Bearbeiten** erlaubt das nachträgliche Ändern von bereits konfigurierten Regelsets.

Wählen Sie **Löschen** um das markierte Regelset zu löschen.

Mit Hilfe der Pfeil-Buttons kann die Position einer Regel innerhalb des aktuellen Regelsets geändert werden.

Bestätigen Sie mit **Speichern**

Bestätigen Sie die angezeigte Meldung mit **Schließen**



Nach erfolgreicher Aktivierung ist das Regelset in der Filterübersicht zu sehen.

Um die Anpassungen zu Aktivieren klicken Sie auf **Aktivieren**.

7.2.5 Neues Regelset auf Layer 3 definieren

Die Konfiguration der Regelsätze in der Filterebene Layer 3 wird auf den folgenden Seiten beschrieben.

Hinweis:

Wenn Sie nach Filterebene Layer 2 konfigurieren möchten, nutzen Sie den Abschnitt **„Neues Regelset auf überbrückten Ethernet-Schnittstellen (Layer 2) definieren“** auf den vorherigen Seiten.

Achtung:

Um ein Regelset auf Layer 3 zu konfigurieren, muss unter dem Pfad: **Grundeinstellungen→ Benutzeroberfläche** ein Haken in der Option: “**Aktiviere IP-Router Funktionen**“ gesetzt werden. Die geänderten Einstellungen müssen nun noch mit „**Aktivieren**“ übernommen werden.

Wählen Sie den Menüpunkt: **Neues Regelset definieren**

Regelset auswählen oder neu erstellen
Regelsets für Layer 3
Allow_L3
Block_L3
ICMP_L3
Log_L3
neues Regelset definieren
Name des Regelsets:
Testregel
Beschreibung des Regelsets:
Testregel
Auf dieser Seite können Sie ein definiertes Regelset auswählen oder ein neues Regelset erstellen. Weiterhin besteht die Möglichkeit ein selbst definiertes zu löschen. Ein vordefiniertes Regelset kann modifiziert werden indem es zuvor mit der Kopieren-Funktion dupliziert wurde.
Ein Regelset kann aus bis zu 10 eigentlichen Filterregeln bestehen.
Momentan aktive Regelsets sind ausgegraut und können nicht verändert werden.
Löschen
Kopieren
Schließen
Weiter

Vergeben Sie einen Namen und eine Beschreibung für das neue Regelset.

Hinweis:

Der Name des Regelsets ist auf 16 Zeichen beschränkt. Leerzeichen, Umlaute und Sonderzeichen können nicht verwendet werden.

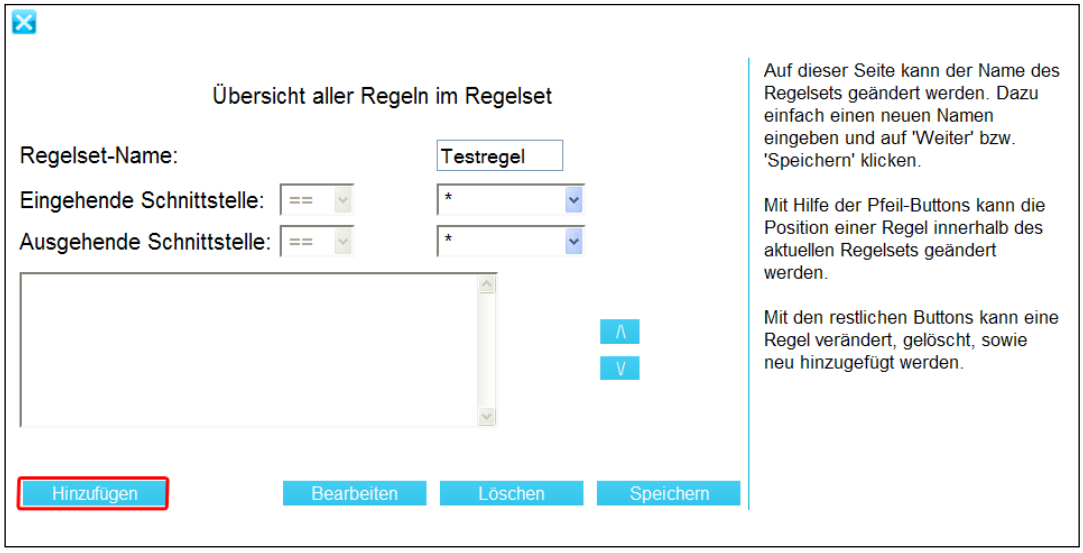
Bestätigen Sie ihre Eingabe mit **Weiter**

LAYER UND SCHNITTSTELLEN DES REGELSETS

Über das Dialogfenster wird die Laufbahn der Pakete eingestellt, auf die dieses Regelset angewendet werden soll. Es wird die eingehende Schnittstelle (auf der die Pakete hereinkommen), sowie die ausgehende Schnittstelle (auf der die Pakete das Gerät nach Akzeptanz verlassen soll) benötigt.

Auf Layer 3 sind je nach Konfiguration folgende Schnittstellen zusätzlich vorhanden:

L3-VPN /Service/IPsec


Übersicht aller Regeln im Regelset
Regelset-Name:
Testregel
Eingehende Schnittstelle:
==
*
Ausgehende Schnittstelle:
==
*
Hinzufügen
Bearbeiten
Löschen
Speichern
Auf dieser Seite kann der Name des Regelsets geändert werden. Dazu einfach einen neuen Namen eingeben und auf 'Weiter' bzw. 'Speichern' klicken.
Mit Hilfe der Pfeil-Buttons kann die Position einer Regel innerhalb des aktuellen Regelsets geändert werden.
Mit den restlichen Buttons kann eine Regel verändert, gelöscht, sowie neu hinzugefügt werden.

BEISPIEL:

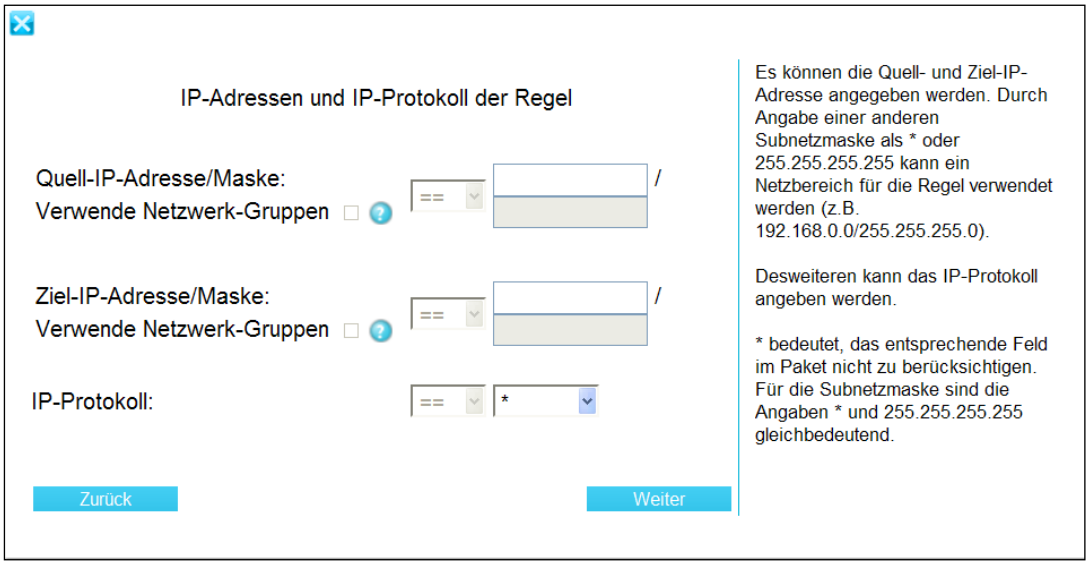
AUSWAHL	SCHNITTSTELLE	FOLGE
==	Eingehende Schnittstelle :**HOST**	filtert alle eingehenden Datenpakete auf dem Port HOST.
!=	Ausgehende Schnittstelle: **WLAN-2**	filtert alle ausgehenden Datenpakete, außer Port WLAN-2

Hinweis:
Wenn Sie keine speziellen Ports filtern möchten, wählen Sie das Sternsymbol welches die Default-Einstellung darstellt.

Bestätigen Sie ihre Eingabe per Klick auf **Weiter**

IP-ADRESSEN UND IP-PROTOKOLL DER REGEL

Die **Quell IP-Adresse** definiert die Adresse des Absenders und die **Ziel IP-Adresse** die des Empfängers.


IP-Adressen und IP-Protokoll der Regel
Quell-IP-Adresse/Maske:
Verwende Netzwerk-Gruppen
Ziel-IP-Adresse/Maske:
Verwende Netzwerk-Gruppen
IP-Protokoll:
==
*
Zurück
Weiter
Es können die Quell- und Ziel-IP-Adresse angegeben werden. Durch Angabe einer anderen Subnetzmaske als * oder 255.255.255.255 kann ein Netzbereich für die Regel verwendet werden (z.B. 192.168.0.0/255.255.255.0).
Desweiteren kann das IP-Protokoll angeben werden.
* bedeutet, das entsprechende Feld im Paket nicht zu berücksichtigen. Für die Subnetzmaske sind die Angaben * und 255.255.255.255 gleichbedeutend.

Hinweis:
Wenn die Option “Verwende Netzwerk-Gruppen“ aktiviert ist, können die hinzugefügten Netzwerk-Gruppen ausgewählt werden. Verwenden Sie diese Option wenn Sie Regeln für mehr als eine IP-Adresse zuweisen möchten.

Hinweis:
Wenn Sie eine dauerhafte Verbindung zwischen zwei fest definierten Geräten verwenden möchten, können Sie die IP-Adressen der jeweiligen Geräte hier festlegen.

Hinweis:
Sobald ein spezielles Protokoll ausgewählt wird, können neue Einstellungen protokollspezifisch getätigt werden.

IP-Protokoll:

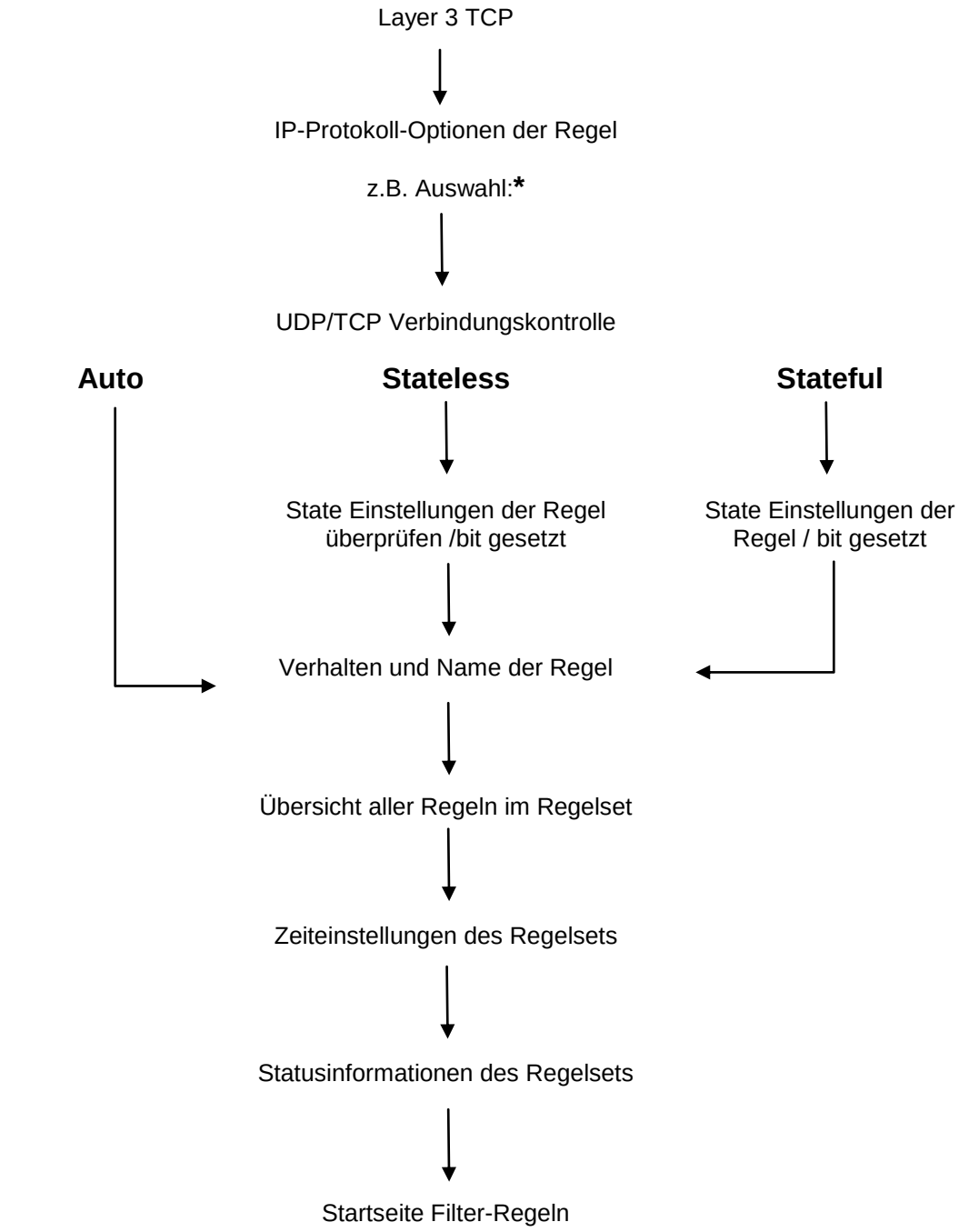
AUSWAHL	FOLGE
TCP	Das Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern.
UDP	Das User Datagram Protocol (Abk. UDP) ist ein minimales, verbindungsloses Netzprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.

ICMP	Das Internet Control Message Protocol (ICMP) benutzt wie TCP und UDP das Internet Protocol (IP), ist also ein Teil der Internetprotokollfamilie. Es dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen.

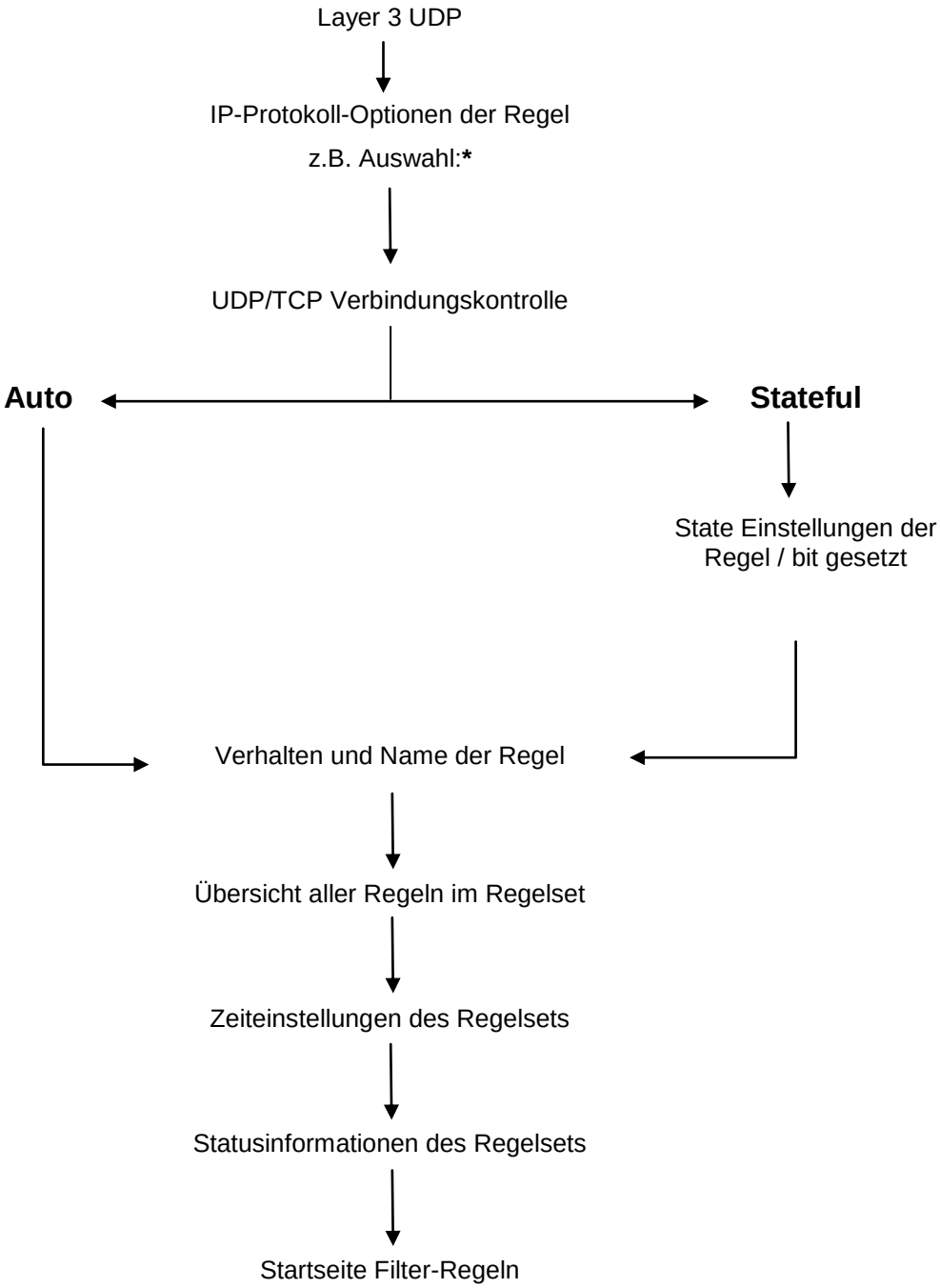
Anhand der folgenden Übersicht können die Konfigurationsmöglichkeiten der Protokolle nachvollzogen werden.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

MENÜÜBERSICHT LAYER 3 AUSWAHL TCP

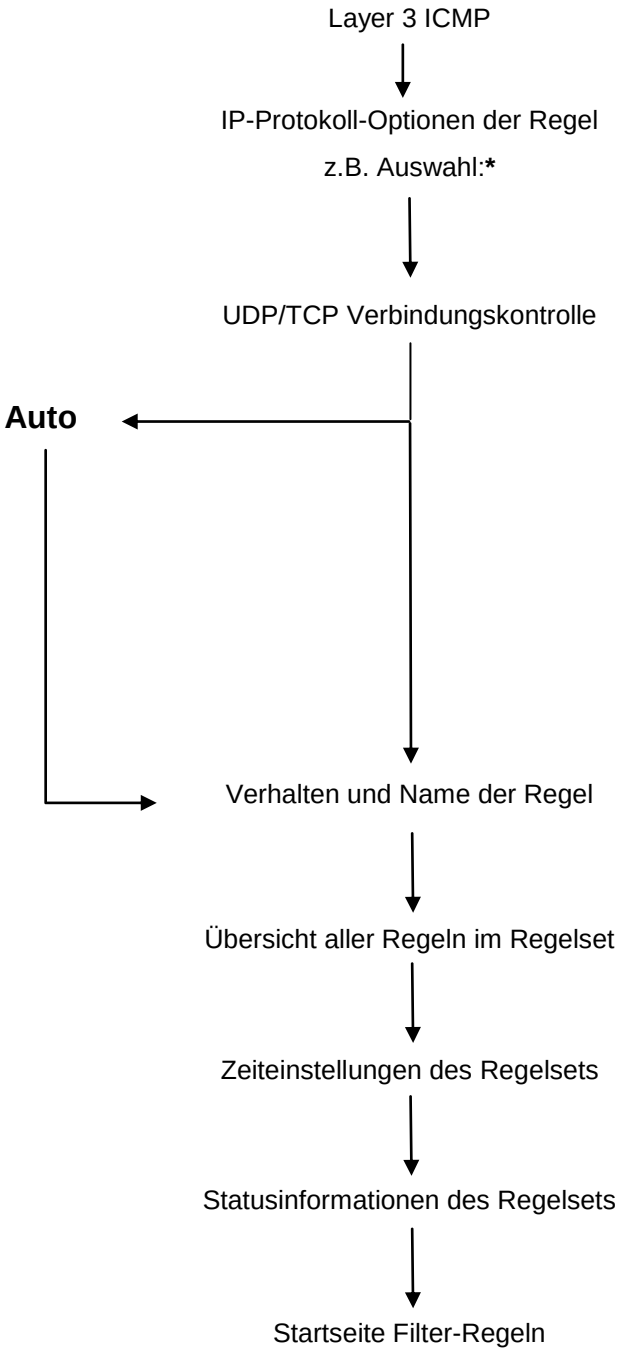


MENÜÜBERSICHT LAYER 3 AUSWAHL UDP



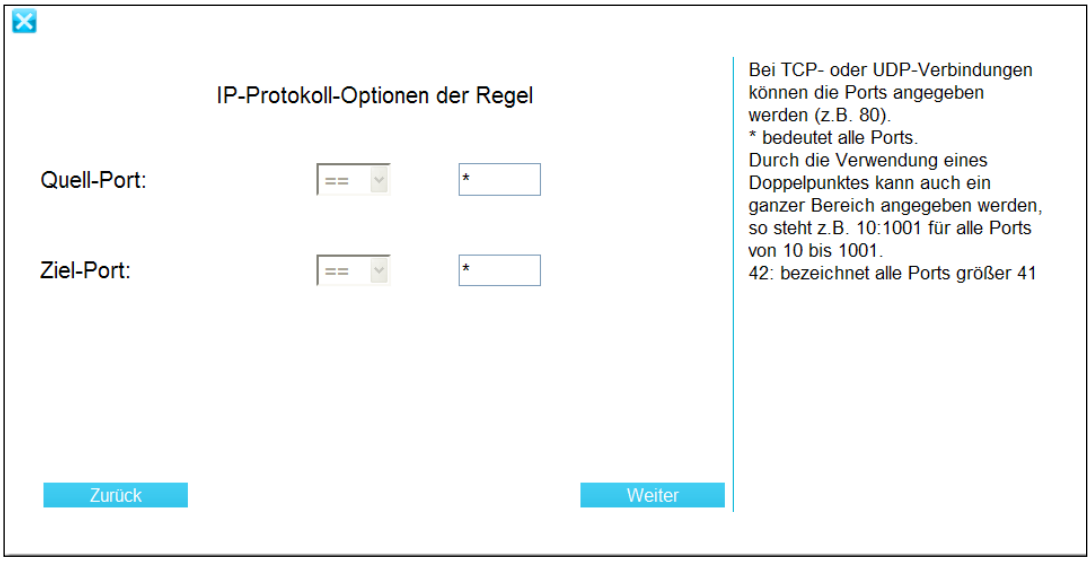
© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

MENÜÜBERSICHT LAYER 3 AUSWAHL ICMP

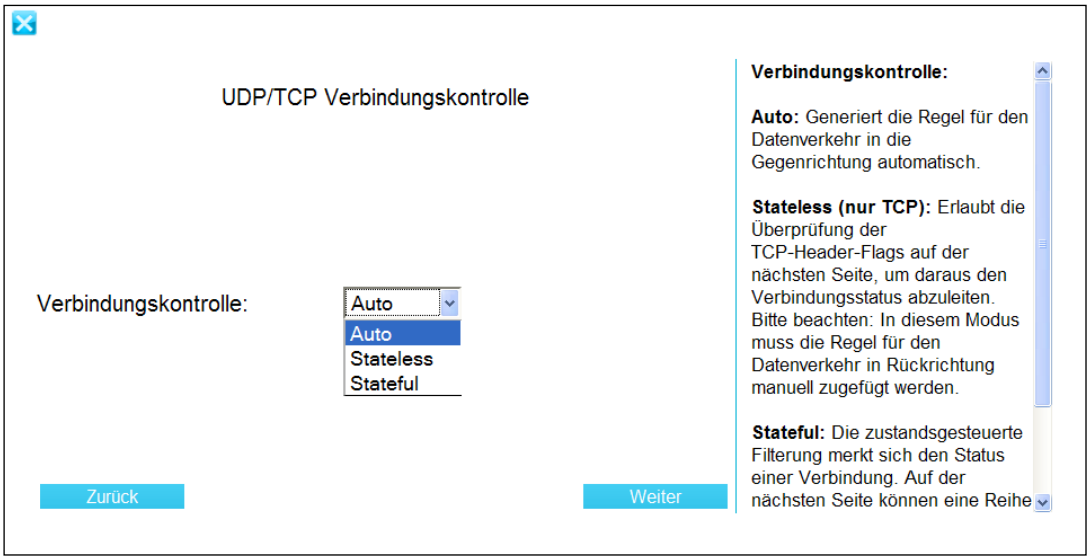


BEISPIELKONFIGURATION AUSWAHL TCP:

Wenn das Protokoll TCP ausgewählt wird, leitet Sie der Assistent durch folgende Menüs:


IP-Protokoll-Optionen der Regel
Quell-Port:
==
*
Ziel-Port:
==
*
Zurück
Weiter
Bei TCP- oder UDP-Verbindungen können die Ports angegeben werden (z.B. 80).
* bedeutet alle Ports.
Durch die Verwendung eines Doppelpunktes kann auch ein ganzer Bereich angegeben werden, so steht z.B. 10:1001 für alle Ports von 10 bis 1001.
42: bezeichnet alle Ports größer 41

Bei TCP-/UDP Verbindungen ist es möglich den Quell-/ Ziel-Port zu definieren. Wenn Sie keine Ports definieren möchten wählen Sie **Weiter**


UDP/TCP Verbindungskontrolle
Verbindungskontrolle:
Auto
Auto
Stateless
Stateful
Zurück
Weiter
Verbindungskontrolle:
Auto: Generiert die Regel für den Datenverkehr in die Gegenrichtung automatisch.
Stateless (nur TCP): Erlaubt die Überprüfung der TCP-Header-Flags auf der nächsten Seite, um daraus den Verbindungsstatus abzuleiten. Bitte beachten: In diesem Modus muss die Regel für den Datenverkehr in Rückrichtung manuell zugefügt werden.
Stateful: Die zustandsgesteuerte Filterung merkt sich den Status einer Verbindung. Auf der nächsten Seite können eine Reihe

Auto Bei TCP/UDP Protokollen wird der Rückweg der Datenpakete automatisch hinzugefügt, lediglich der Verbindungsaufbau der Regel muss spezifiziert werden.

Stateless: Nur bei TCP:Die TCP Flags wie ACK, SYN, FIN usw. können manuell spezifiziert werden.

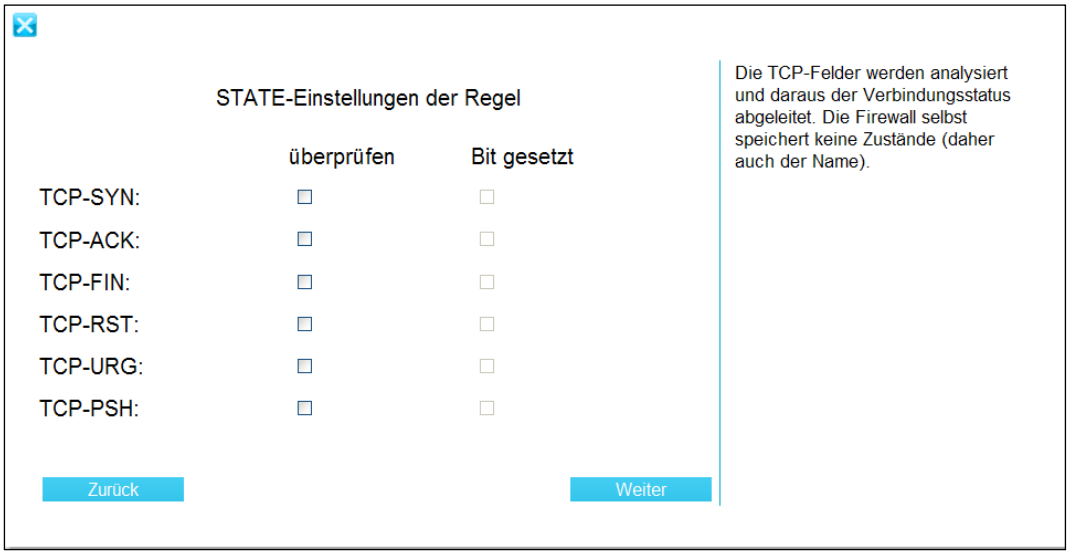
Stateful: Es können verschieden Einstellungen wie State Related, State New, State Established und State Invalid gesetzt werden. Die manuelle Auswahl von TCP Flags ist nicht möglich. Das Gerät verwendet in diesem Fall eine Protokollanalyse, um den Verbindungszustand einer TCP Verbindung oder auch einer Layer 6 Datenverbindung wie FTP zu detektieren.

AUTO

Wenn die Auswahl Auto gewählt wird, gelangen Sie zum Menü Verhalten und Name der Regel.

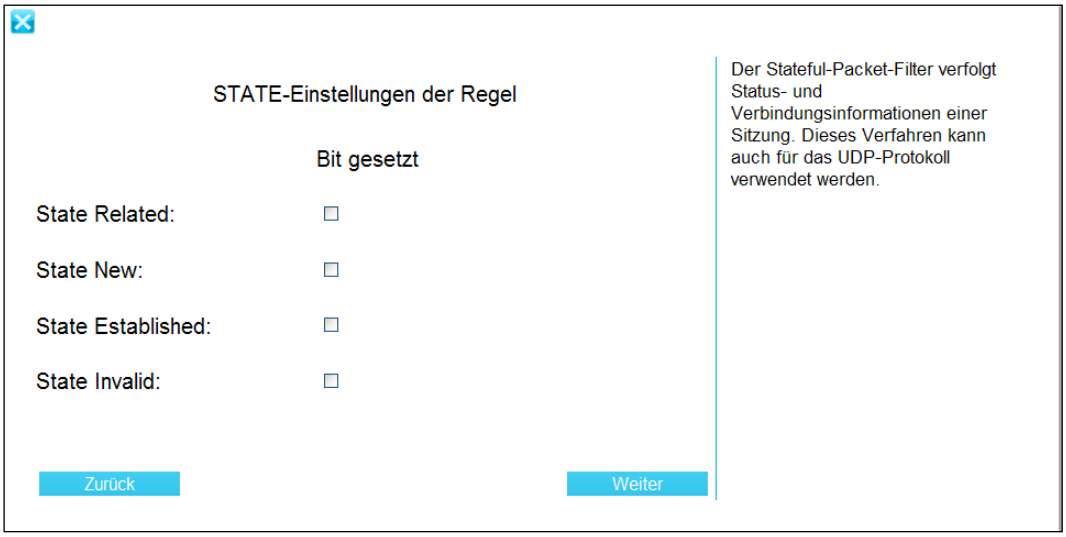
STATELESS:

Bei eingeschalteter Funktion werden die TCP Felder analysiert, aus dem der Verbindungsstatus abgeleitet wird.



STATEFUL:

Der Stateful-Packetfilter verfolgt Verbindungsinformationen einer Sitzung.



State Related: Datenpaket ist einer bestehenden Datenverbindung zugeordnet, z.B, Aufbau eines FTP-Rückkanals.

State New: Datenpaket baut eine neu Datenverbindung auf, z.B. TCP mit SYN-Flag.

State Established: Datenpaket ist direkt einer bestimmten Datenverbindung zugehörig, z.B. TCP Daten ohne SYN- Flag.

State Invalid: Datenpakete für welche das Gerät keinen gültigen Verbindungszustand festlegen konnte.

AKTION UND NAME DER REGEL

Im Dialogfenster kann das Verhalten der Regel definiert werden. Unter dem Menüpunkt Aktion für die Regel können Sie festlegen, wie das Gerät mit einem Paket verfahren soll. Des Weiteren können die Events protokolliert werden, es kann ein Alarm ausgelöst werden und der Datendurchsatz beschränkt werden.

Aktion für die Regel:
Zur Auswahl stehen:

Zulassen: Das Paket wird weitergeleitet.

Verwerfen: Das Paket wird ohne Nachricht an den Absender gelöscht.

Abweisungsgrund:
Hier kann der Abweisungsgrund definiert werden, der dem Absender gemeldet wird.

Log:
Es wird ein Eintrag im Eventlog protokolliert.

Alarm:
Es wird der Alarmausgang gesetzt.

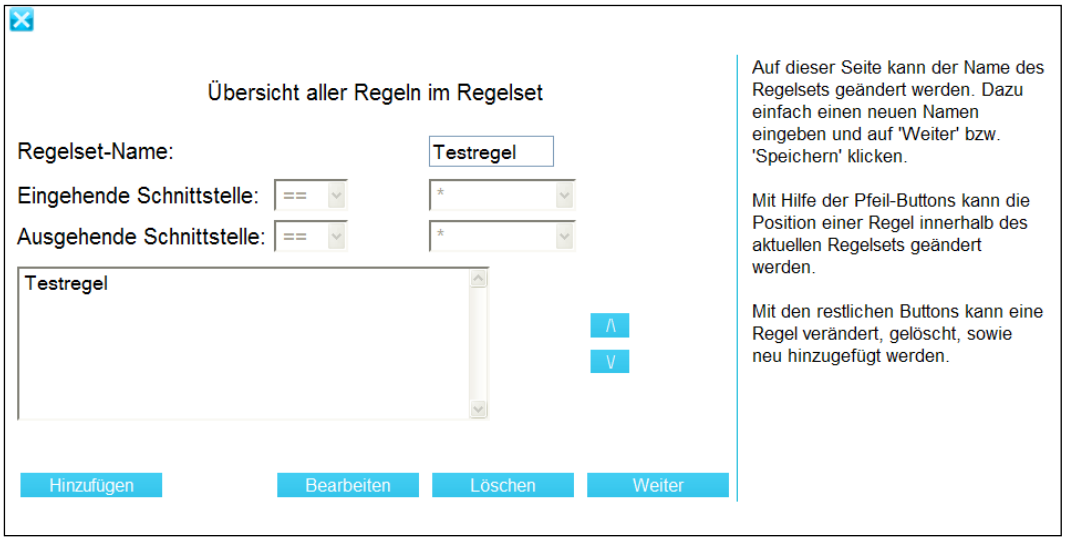
Max.Pakete/Sek:
Hier kann die maximale Paketrate pro Sekunde festgelegt werden, die als Obergrenze gegen einen Denial-of-Service eingestellt werden kann. Dies ist ebenfalls sinnvoll, um Regeln die in einem häufigen Intervall einen Eventlogeintrag erzeugen würden, zu begrenzen

Name der Regel:
Definieren Sie einen eindeutigen Regelnamen. Es ist zwingend notwendig, dass Sie einen Namen für die Regel des Regelsets vergeben.

Bestätigen Sie mit: **Weiter**

ÜBERSICHT ALLER REGELN EINES REGELSETS:

Das Dialogfenster zeigt die einzelnen Regeln des Regelsets an. Diese können in ihrer Reihenfolge geändert werden. Des Weiteren kann der Regelsetname geändert werden.



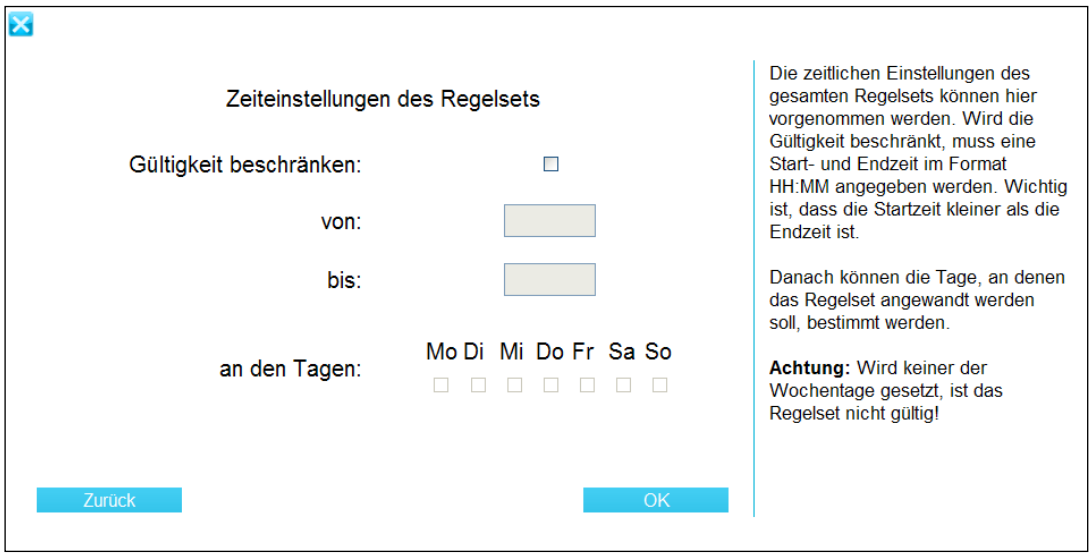
Über den Button **Hinzufügen** startet der Einrichtungsprozess erneut und eine neue Regel kann definiert werden. Der Button **Bearbeiten** erlaubt das nachträgliche Ändern von bereits erstellten Regeln.

Wählen Sie **Löschen,** um das markierte Regel zu löschen.

Mit Hilfe der Pfeil-Buttons kann die Position einer Regel innerhalb des aktuellen Regelsets geändert werden.

Bestätigen Sie mit: **Weiter**

ZEITEINSTELLUNGEN DES REGELSETS


Zeiteinstellungen des Regelsets
Gültigkeit beschränken:
von:
bis:
an den Tagen:
Mo Di Mi Do Fr Sa So
Zurück
OK
Die zeitlichen Einstellungen des gesamten Regelsets können hier vorgenommen werden. Wird die Gültigkeit beschränkt, muss eine Start- und Endzeit im Format HH:MM angegeben werden. Wichtig ist, dass die Startzeit kleiner als die Endzeit ist.
Danach können die Tage, an denen das Regelset angewandt werden soll, bestimmt werden.
Achtung: Wird keiner der Wochentage gesetzt, ist das Regelset nicht gültig!

Hinweis:
Wurde die Gültigkeit beschränkt muss mindestens ein Wochentag angegeben werden, ansonsten ist die Regel ungültig und wird nicht verwendet.

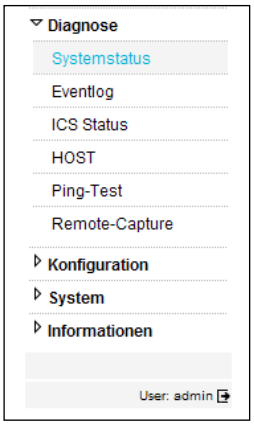
Hinweis:
Unabhängig von der Zeitzonenkonfiguration des Gerätes müssen die Gültigkeitszeiträume unter Berücksichtigung der UTC-Zeit konfiguriert werden!

Schliessen Sie die Konfiguration mit **Speichern** ab.
Bestätigen Sie die angezeigte Meldung mit **Schließen**

Nach erfolgreicher Aktivierung ist das Regelset in der Filterübersicht zu sehen. Um die Anpassungen zu aktivieren klicken Sie auf **Aktivieren**.

8 ACCESS POINT/CLIENT WEBOBERFLÄCHE

Das Webinterface des Access Points gliedert sich in fünf Hauptmenüpunkte auf.



DIAGNOSE

Zeigt den aktuellen Status der Schnittstellen

KONFIGURATION

Konfiguriert die Access Point- spezifischen Funktionen

SYSTEM

Erlaubt grundlegende Einstellungen und Änderungen im Webinterface

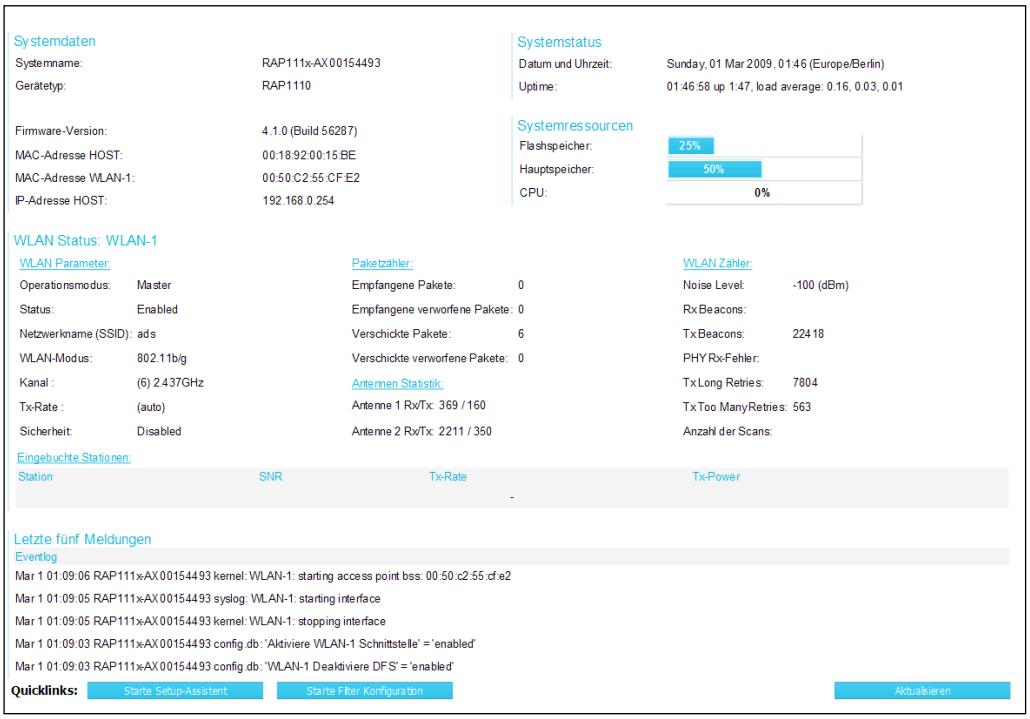
INFORMATIONEN

Enthält Allgemeine Informationen zum Gerät

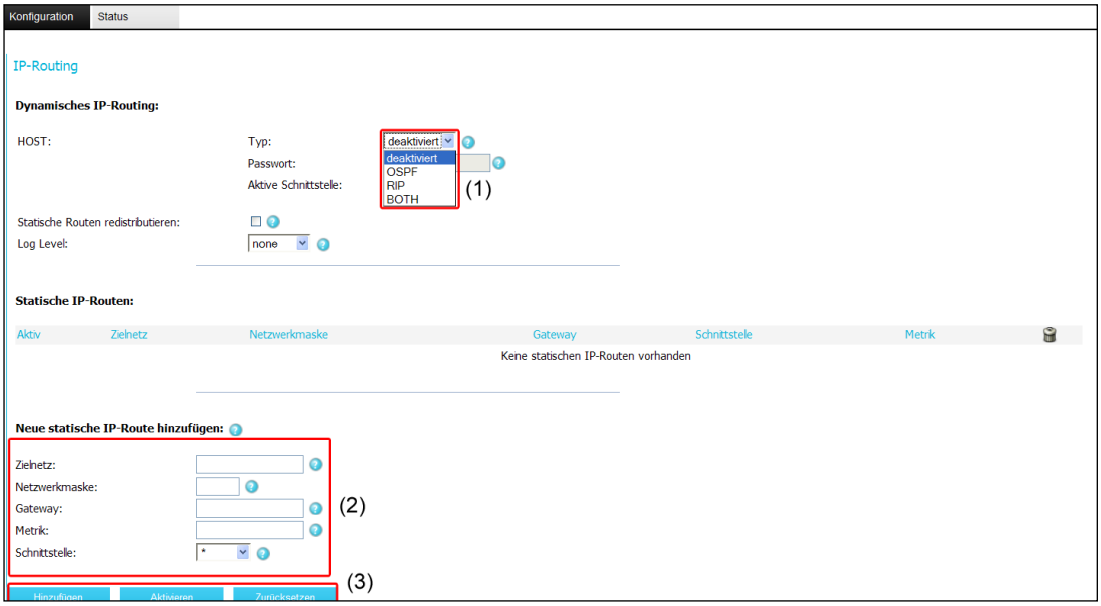
8.1 HAUPTMENÜPUNKT DIAGNOSE

8.1.1 SYSTEMSTATUS

Die Startseite des Webinterfaces zeigt alle wichtigen Einstellungen des Access Points auf einen Blick. Die Funktionen lassen sich über einen Hyperlink direkt von der Startseite aus anwählen.

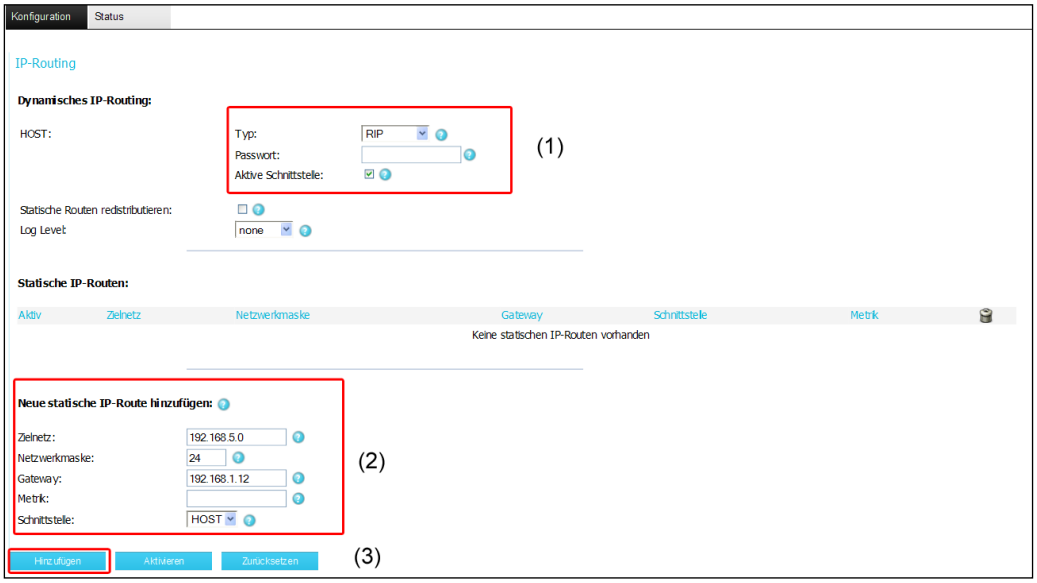


8.2 ALLGEMEINE ÜBERSICHT ZUR KONFIGURATION IN DEN MENÜS



8.2.1 BEISPIELKONFIGURATION IP-ROUTING

Das Beispiel zeigt anhand des Menüpunkts IP-Routing wie eine Einstellung gemacht und übernommen wird. Außerdem wird erläutert wie eine Einstellung deaktiviert, bzw. gelöscht wird.



Hinweis:

Wenn Sie bei Auswahl / Eingabefeldern nicht genau wissen welche Einstellung die Richtige ist, können Sie mit der Maus auf das Fragezeichen neben der Auswahl gehen. Es erscheint eine Hinweisbox mit Tipps und Erklärungen, sowie einigen Beispielen.

AUSWAHL 1

Treffen Sie zunächst eine Auswahl im Dropdown-Menü. Klicken Sie dazu auf den Pfeil neben der Einstellung um eine Auswahl zu treffen.

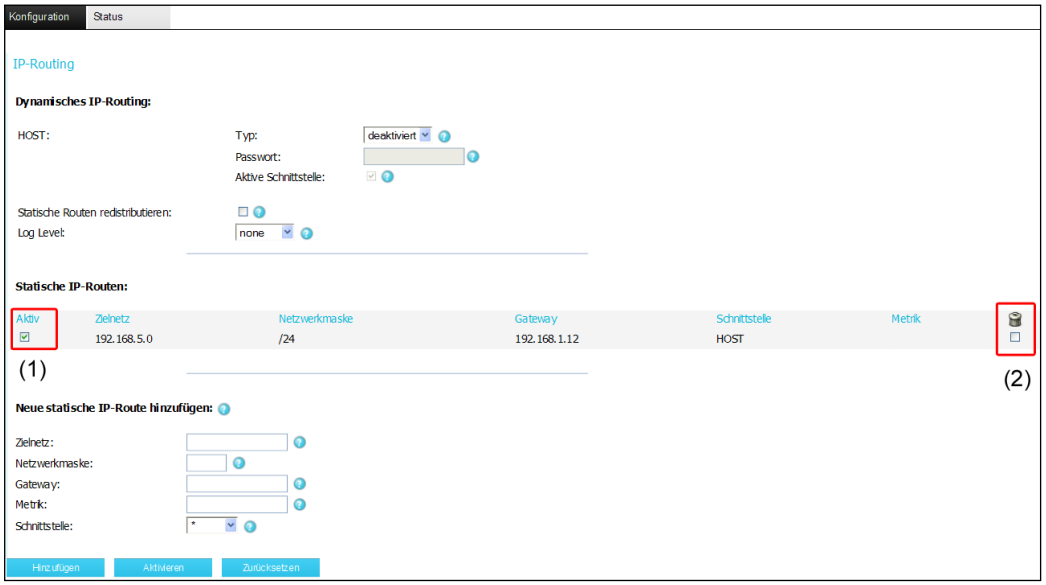
AUSWAHL 2

Tragen Sie anschließend alle benutzerspezifischen Einstellungen in die Eingabefelder ein.

AUSWAHL 3

Bestätigen Sie ihre Eingaben per Klick auf „**Hinzufügen**“. Ihre Einstellungen werden nun übernommen.

Ihre Eingaben wurden nun übernommen und sind aktiviert. (Haken bei 1)



AUSWAHL 1

Wenn Sie eine aktivierte Einstellung deaktivieren möchten, entfernen Sie den Haken bei 1 und wählen „**Aktivieren**“. Die Einstellung wird nun deaktiviert.

AUSWAHL 2

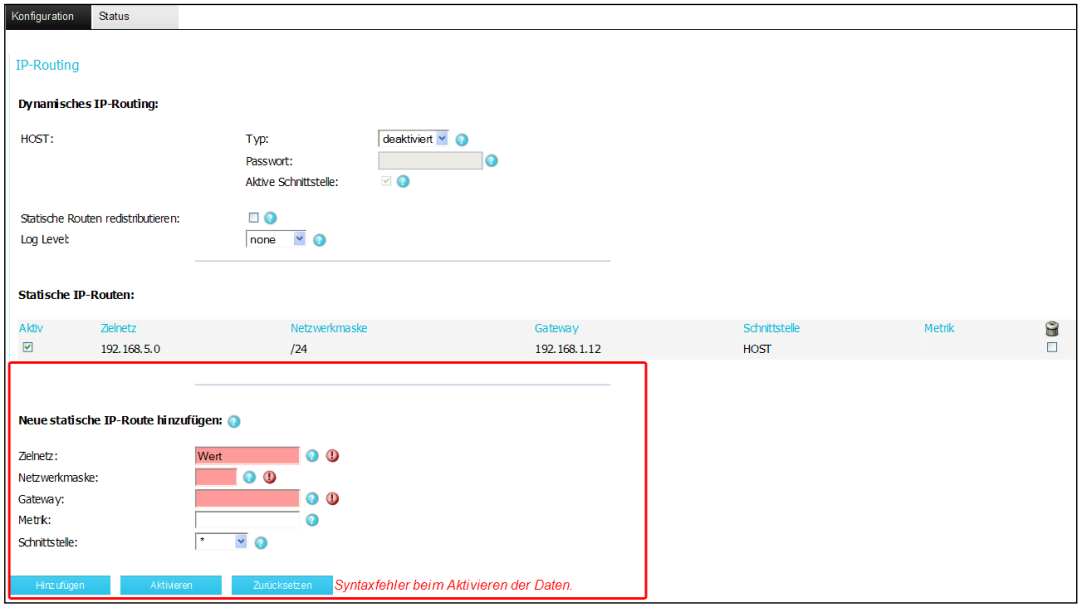
Um eine Einstellung zu löschen setzen Sie den Haken bei 2 und wählen „**Aktivieren**“.

Hinweis:

Der Button „Zurücksetzen“ in der Schaltflächenleiste erlaubt es gerade getätigte Einstellungen auf den Default-Wert zurückzusetzen.

8.2.2 FEHLERMELDUNGEN

Falsche Eingaben kennzeichnet das Gerät durch rot hervorgehobene Eingabefelder.



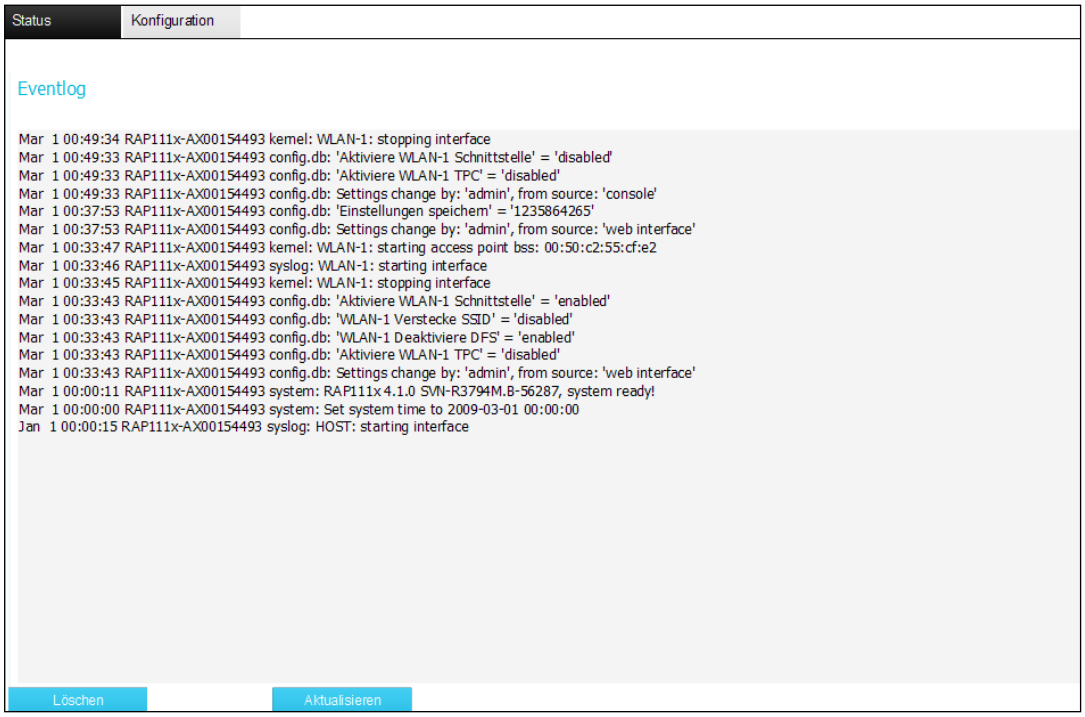
Hinweis:

Anhand des Ausrufezeichens neben der Falscheingabe kann ermittelt werden was die Ursache für den Fehler sein kann, bzw. welche Werte verlangt werden.

8.2.3 EVENTLOG

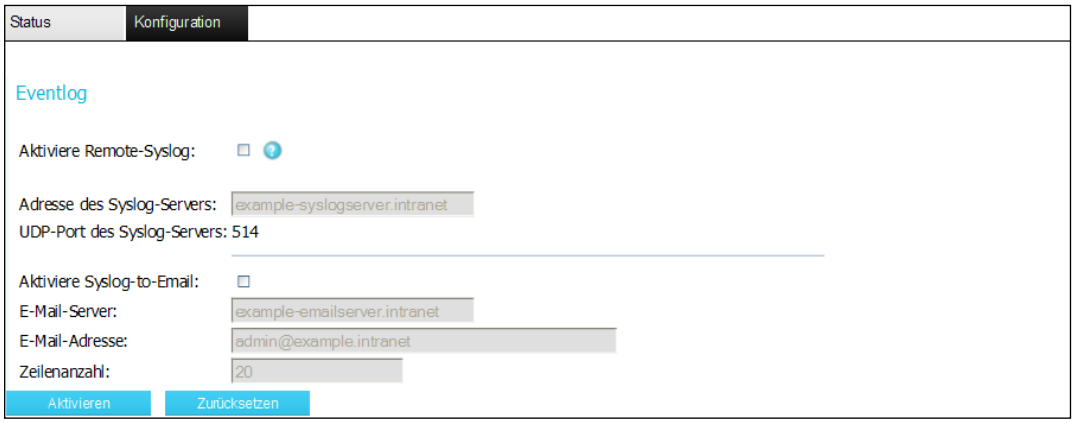
STATUS

Der Eventlog stellt das wichtigste Diagnosewerkzeug des Geräts dar und enthält essentielle Informationen zum Systemzustand. Hier werden eventuelle Fehlermeldungen des Systems eingetragen und dargestellt. Die Eventlog-Anzeige verhält sich wie ein Protokoll und zeichnet alle Systemaktivitäten auf. Geänderte Einstellungen oder Fehlermeldungen können hier als Protokoll eingesehen werden.


Status
Konfiguration
Eventlog
Mar 1 00:49:34 RAP111x-AX00154493 kernel: WLAN-1: stopping interface
Mar 1 00:49:33 RAP111x-AX00154493 config.db: 'Aktiviere WLAN-1 Schnittstelle' = 'disabled'
Mar 1 00:49:33 RAP111x-AX00154493 config.db: 'Aktiviere WLAN-1 TPC' = 'disabled'
Mar 1 00:49:33 RAP111x-AX00154493 config.db: Settings change by: 'admin', from source: 'console'
Mar 1 00:37:53 RAP111x-AX00154493 config.db: 'Einstellungen speichern' = '1235864265'
Mar 1 00:37:53 RAP111x-AX00154493 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:33:47 RAP111x-AX00154493 kernel: WLAN-1: starting access point bss: 00:50:c2:55:cf:e2
Mar 1 00:33:46 RAP111x-AX00154493 syslog: WLAN-1: starting interface
Mar 1 00:33:45 RAP111x-AX00154493 kernel: WLAN-1: stopping interface
Mar 1 00:33:43 RAP111x-AX00154493 config.db: 'Aktiviere WLAN-1 Schnittstelle' = 'enabled'
Mar 1 00:33:43 RAP111x-AX00154493 config.db: 'WLAN-1 Verstecke SSID' = 'disabled'
Mar 1 00:33:43 RAP111x-AX00154493 config.db: 'WLAN-1 Deaktiviere DFS' = 'enabled'
Mar 1 00:33:43 RAP111x-AX00154493 config.db: 'Aktiviere WLAN-1 TPC' = 'disabled'
Mar 1 00:33:43 RAP111x-AX00154493 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:00:11 RAP111x-AX00154493 system: RAP111x 4.1.0 SVN-R3794M.B-56287, system ready!
Mar 1 00:00:00 RAP111x-AX00154493 system: Set system time to 2009-03-01 00:00:00
Jan 1 00:00:15 RAP111x-AX00154493 syslog: HOST: starting interface
Löschen
Aktualisieren

KONFIGURATION

Das Protokoll des Eventlog kann ebenfalls bequem auf einen zentralen Rechner gesendet werden. Hierzu wird der Remoterechner in den Eingabefeldern eingetragen.

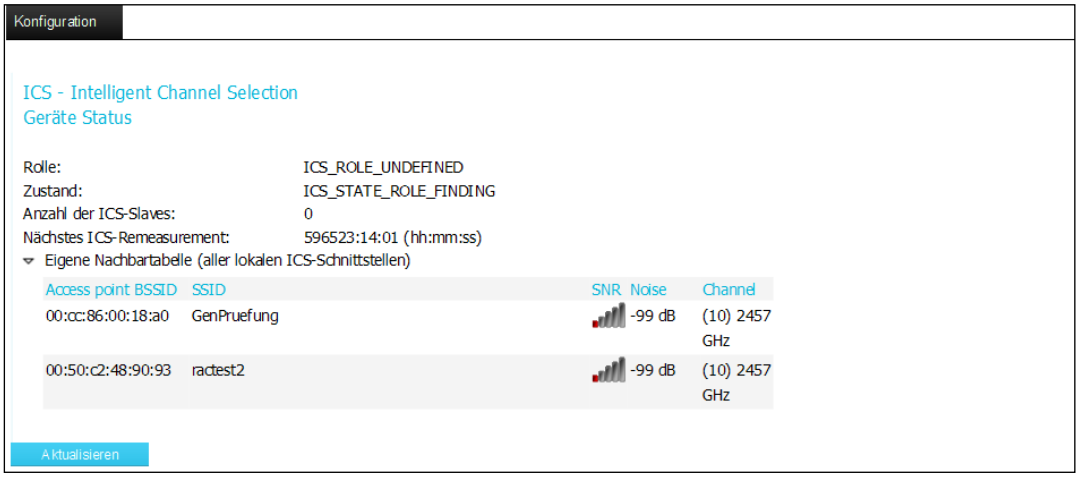


Zusätzlich ist das Versenden der Syslog-Nachrichten per E-Mail möglich. Spezifizieren sie hierzu die IP-Adresse des E-Mail-Servers sowie eine Empfängeradresse.

Hinweis:

Um ein hohes Datenaufkommen von E-Mails zu verhindern ist die Eingabe eines geeigneten Schwellenwerts im Feld Zeilenanzahl zu empfehlen. Die Zeilenanzahl spezifiziert die Anzahl der Zeilen die bei Erreichen des Schwellenwerts in einer E-Mail zusammen versendet werden.

8.2.4 ICS-STATUS



Der Menüpunkt ICS-Status gibt Aufschluss über sämtliche in der Nähe befindlichen Netzwerkstrukturen. Über **Eigene Nachbartabelle** können diese detallierter angezeigt werden.

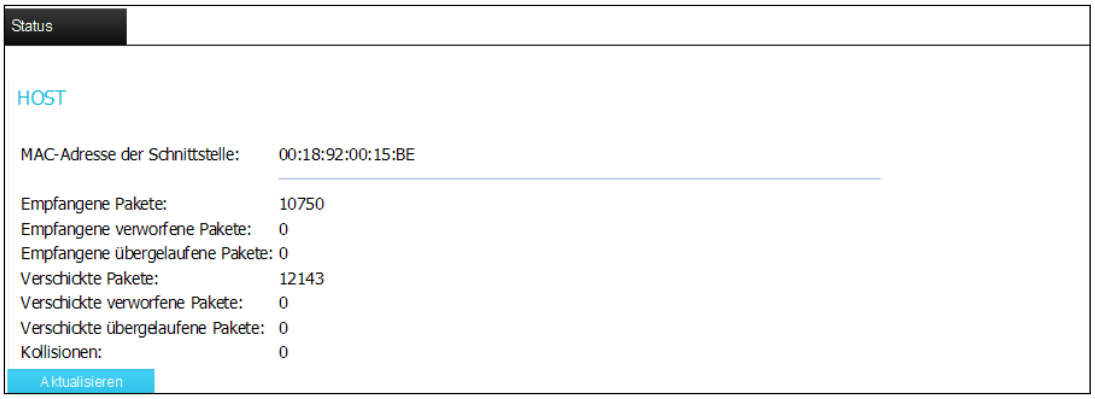
Hinweis:

Um die ICS-Funktion zu aktivieren, muss unter **Konfiguration → WLAN-1/2-Parameter → Kanal**, die Einstellung **ICS** aktiviert sein.

Hinweis:

Weitere Informationen über die Funktionsweise von ICS, werden im Kapitel WLAN Konfiguration beschrieben.

8.2.5 HOST



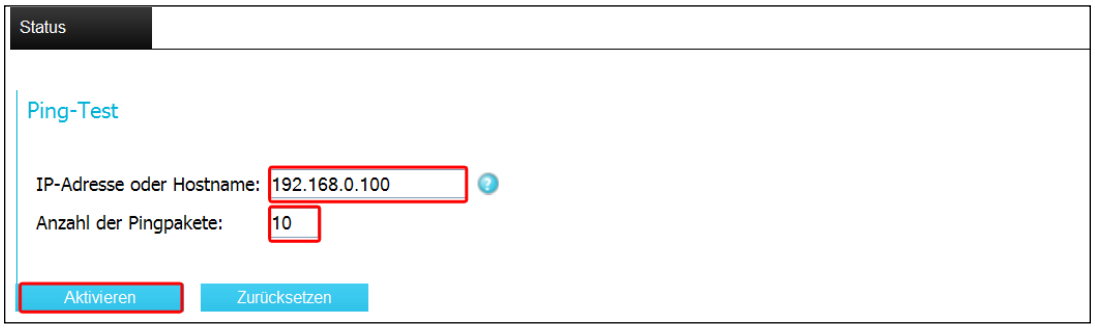
Anhand der Daten kann genau nachvollzogen werden wie Pakete empfangen, bzw. verschickt wurden. Die Anzeige kann über Aktualisieren auf den neuesten Stand gebracht werden.

8.2.6 Ping Test

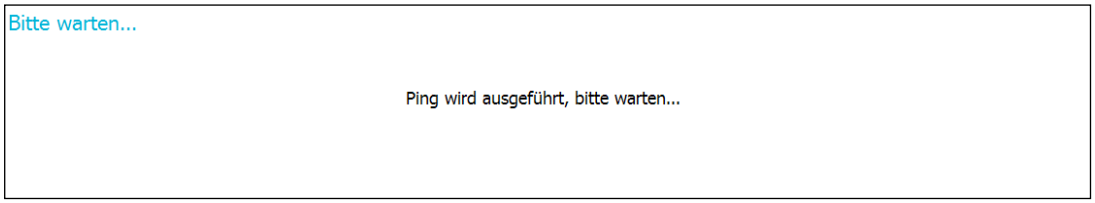
Mit Hilfe des Ping-Tests kann die Erreichbarkeit einer angeschlossenen Gegenstelle überprüft werden. Der Ping-Test sendet ein Echo-Request-Paket an die Zieladresse der zu überprüfenden Gegenstelle und wertet die Informationen des Tests aus.

Geben Sie die zu überprüfende Zieladresse in Form der IP-Adresse im dafür vorgesehenen Feld ein. Zusätzlich muss die zu sendende Paketanzahl angegeben werden. Diese ist auf maximal 10 Pakete begrenzt.

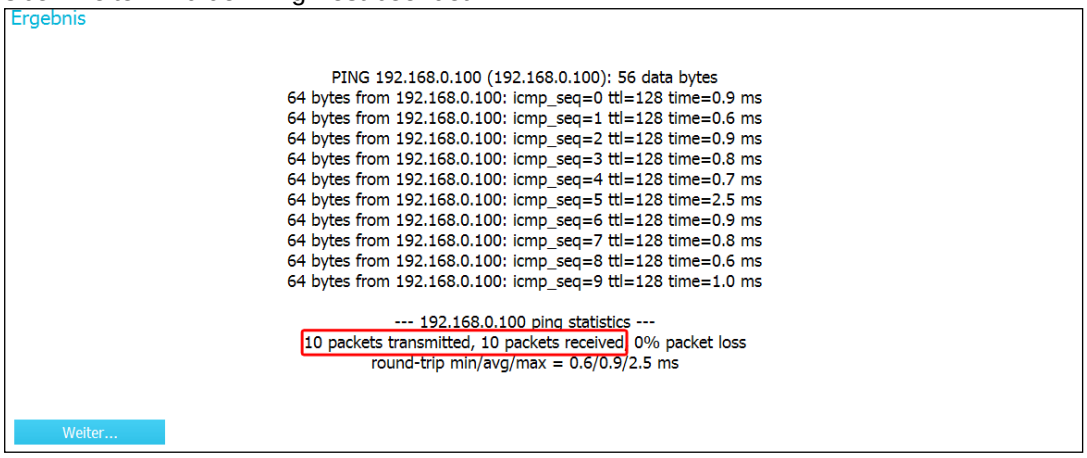
Per Klick auf **Aktivieren** startet der Ping Test.



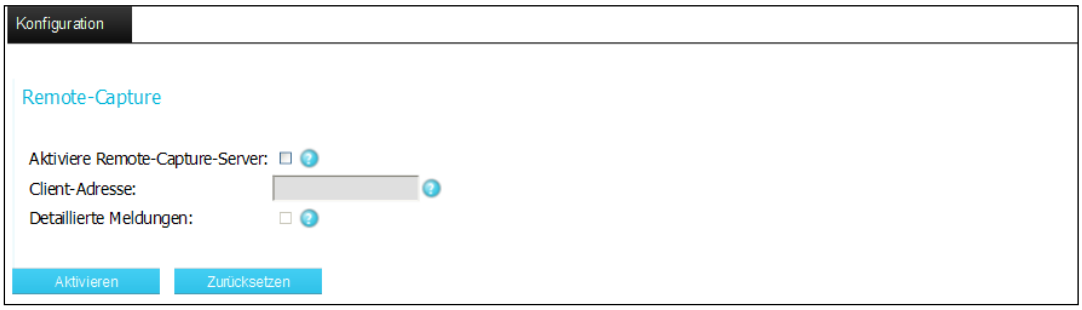
Nach kurzer Zeit erscheint eine Übersicht, welche den Verlauf und das Ergebnis des Ping Tests darstellt. Die Übersicht zeigt sowohl den gesendeten, als auch den erhaltenen Paketstatus.



Über Weiter wird der Ping Test beendet.


Ergebnis
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=128 time=0.9 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=128 time=0.8 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=128 time=0.7 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=128 time=2.5 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=128 time=0.9 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=128 time=0.8 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=128 time=0.6 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=128 time=1.0 ms
--- 192.168.0.100 ping statistics ---
10 packets transmitted, 10 packets received 0% packet loss
round-trip min/avg/max = 0.6/0.9/2.5 ms
Weiter...

8.2.7 REMOTE CAPTURE



Mit Remote Capture können die Datenpakete der einzelnen Schnittstellen des Access Point zu Diagnosezwecken aufgezeichnet werden. Dazu ist es nötig unter Windows das Tool „**Wireshark**“ zu verwenden. Zusätzlich ist es möglich die WLAN Schnittstellen in den Monitor Modus setzen und auf 802.11 Ebene Pakete mit dem Tool Radiotap Header aufzuzeichnen.

8.3 HAUPTMENÜPUNKT KONFIGURATION

8.3.1 IP-KONFIGURATION

Unter **IP-Konfiguration** kann der Betriebsmodus eingestellt werden.

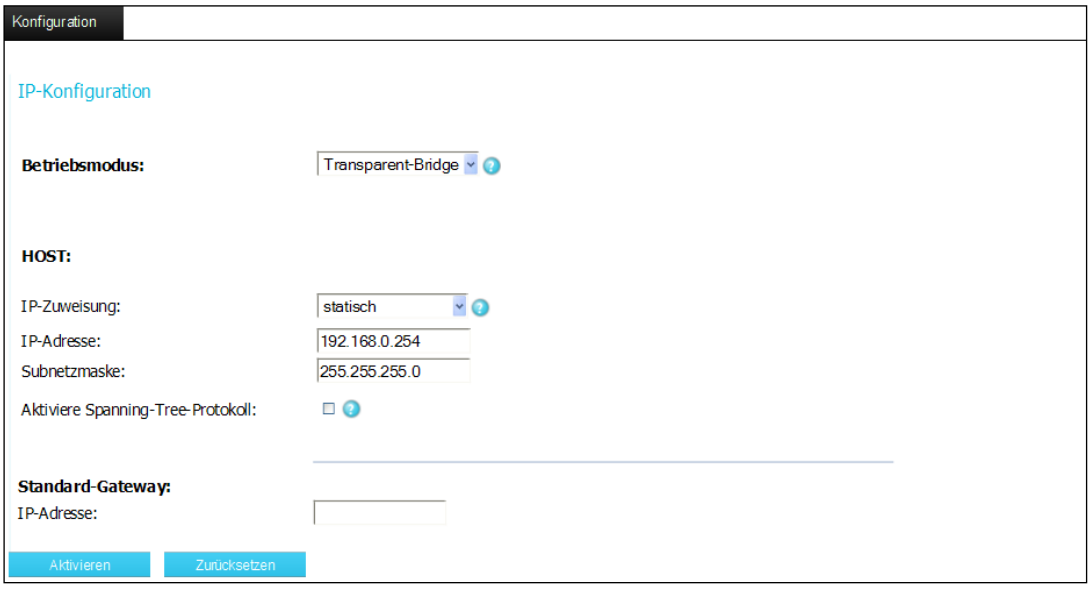
Folgende Betriebsmodi stehen zur Verfügung: Transparent-Bridge und IP-Router.

Über Transparent-Bridge können Sie den Access Point in eine bestehende Netzwerkstruktur integrieren, ohne in diesem Anpassungen vorzunehmen. Das Gerät ist für die bestehende Netzwerkstruktur unsichtbar.

Über IP-Router teilt das Gerät das Netz in zwei getrennte Teilnetze auf. Diese Einstellung erfordert ggf. eine Anpassung der vorhandenen Netzwerkstrukturen.

Alle Betriebsmodi unterscheiden sich in ihrer Konfiguration.

TRANSPARENT-BRIDGE



Hinweis:

Das Fragezeichen rechts neben dem Drop- Down Menü gibt Ihnen Hinweise und Kurzerklärungen zu den zur Auswahl stehenden Menüpunkten.

Statisch:

Wenn diese Option gewählt ist kann eine fest zugewiesene IP-Adresse eingetragen werden.

Die statische IP-Zuweisung erfordert die Eingabe der IP-Adresse und der Subnetzmaske.

Die Default Werte sind:

IP-Adresse: **192.168.0.254**

Subnetzmaske: **255.255.255.0**

DHCP:

Die DHCP Funktion fordert eine IP-Adresse von einem DHCP- Server an und nimmt die Zuweisung automatisch vor.

DHCP rückfallend:

Die Option ist eine Kombination aus statischer und automatischer Zuweisung der IP-Adresse. Sollte ein Fehler bei der automatischen Zuweisung des DHCP Servers auftreten oder kein DHCP-Server zur Verfügung stehen, wechselt die IP-Zuweisung automatisch auf die eingetragene statische IP.

Aktiviere Spanning Tree Protokoll:

Das Spanning Tree Protokoll dient zur Vermeidung von Kreisläufen (Schleifen), speziell in geswitchten Netzwerkumgebungen.

Bei aktivierter Funktion ist es möglich redundante Netzwerkleitungen zu erzeugen.

Standard-Gateway

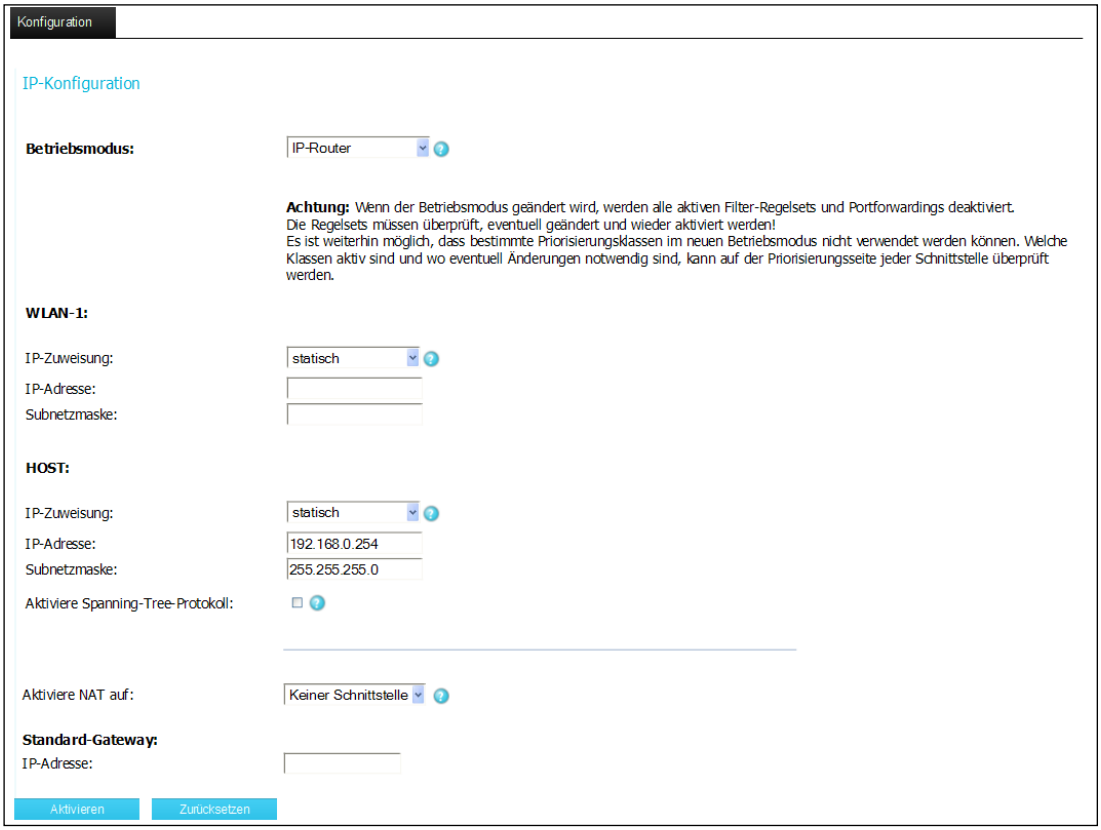
Hier kann die IP-Adresse des zu verwendenden Gateways eingetragen werden.

Die IP-Adresse des Standard-Gateways dient dem Gerät dazu eine IP-Konfiguration zu einer Adresse außerhalb seines eigenen IP-Subnetzes aufzubauen (im Beispiel außerhalb 192.168.0.254). Die IP-Adresse selbst muss jedoch innerhalb dieses Netz-Bereiches liegen. Der Wert wird evtl. durch einen dynamischen DHCP Wert überschrieben, falls unter IP-Zuweisung DHCP konfiguriert wurde und der DHCP Server diese Option Unterstützt. Der Standard-Gateway kann nötig sein um z.B. einen NTP Zeitserver zu erreichen oder um die IP-Adresse wiederum selbst bei einer DHCP Server Einstellung an WLAN-Clients weiterzugeben.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

IP-ROUTER

Die Auswahl IP-Router teilt die Netze zwischen HOST und HOST Schnittstelle in zwei separate Netze auf und filtert diese separat.



Schnittstelle HOST:

Die IP-Zuweisung der HOST Schnittstelle kann auf folgende Arten erfolgen:

Statisch:

Wenn diese Option gewählt ist, kann eine fest zugewiesene IP-Adresse eingetragen werden.

Die statische IP-Zuweisung erfordert die Eingabe der IP-Adresse und der Subnetzmaske.

Die Default Werte sind:

IP-Adresse: **192.168.0.254**

Subnetzmaske: **255.255.255.0**

DHCP:

Die DHCP Funktion fordert eine IP-Adresse von einem DHCP- Server an und weist Sie automatisch dem Gerät zu.

DHCP rückfallend:

Die Option ist eine Kombination aus statischer und automatischer Zuweisung der IP-Adresse. Sollte ein Fehler bei der automatischen Zuweisung des DHCP Servers auftreten oder kein DHCP-Server zur Verfügung stehen, wechselt die IP-Zuweisung automatisch auf die eingetragene statische IP.

PPPoE / DHCP

Die IP-Adresse der **P**oint to **P**oint **P**rotocol **o**ver **E**thernet-Verbindung wird dynamisch vom System zugewiesen. Diese Auswahl ist die klassische Einstellung für ADSL-Einwahlverbindungen bei denen der Provider die IP-Adresse dynamisch zuweist.

Der PPPoE Benutzername enthält die vom Provider vorgegebenen Anmeldedaten.

Aktiviere Spanning Tree Protokoll:

Das Spanning Tree Protokoll dient zur Vermeidung von Kreisläufen (Schleifen), speziell in geswitchten Netzwerkumgebungen. Bei aktivierter Funktion ist es möglich, redundante Netzwerkleitungen zu erzeugen.

Aktiviere NAT auf:

Durch die Aktivierung der Network Adress Translation (NAT) wird auf der ausgewählten Schnittstelle ein privater IP-Adressbereich mit einer globalen IP-Adresse maskiert werden. Die Aktivierung von NAT wird bei DSL/PPoE Verbindungen empfohlen.

Standard-Gateway:

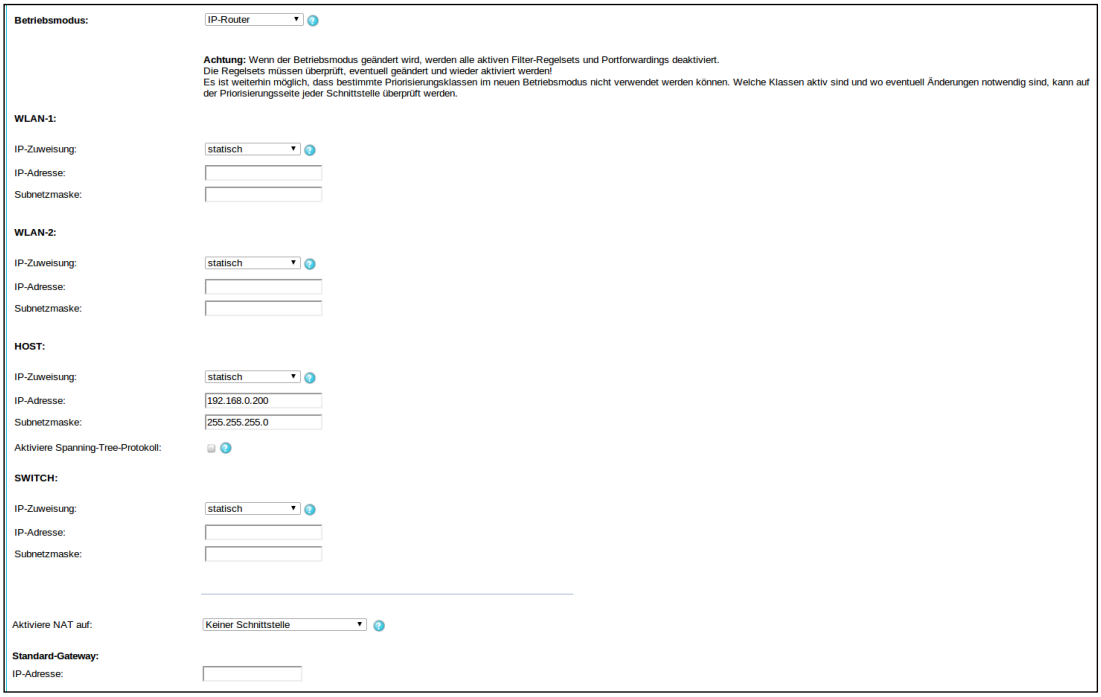
Hier kann die IP-Adresse des verwendeten Gateways angegeben werden.

Es folgt ein Klick auf **Aktivieren.** Ihre Änderungen sind nun aktiviert.

Hinweis:

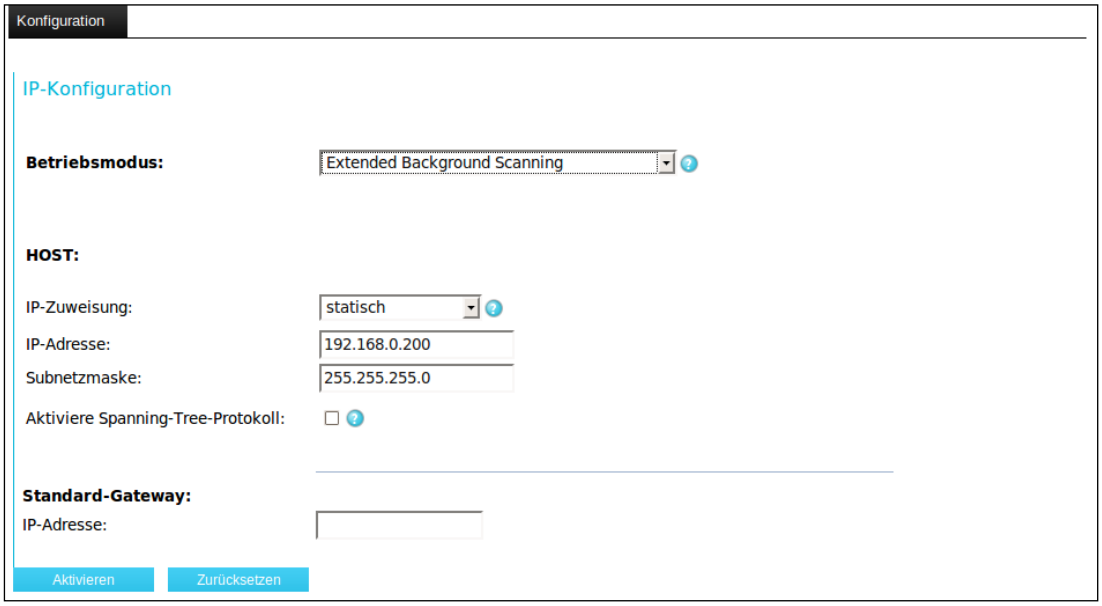
Die folgenden Konfigurationsmöglichkeiten sind nur bei entsprechender Ausstattungsvariante vorhanden.

IP-KONFIGURATION (RAC15XX)



Das Gerät RAC15xx verfügt über einen eingebauten Switch, welcher in der IP-Konfiguration konfigurierbar ist.

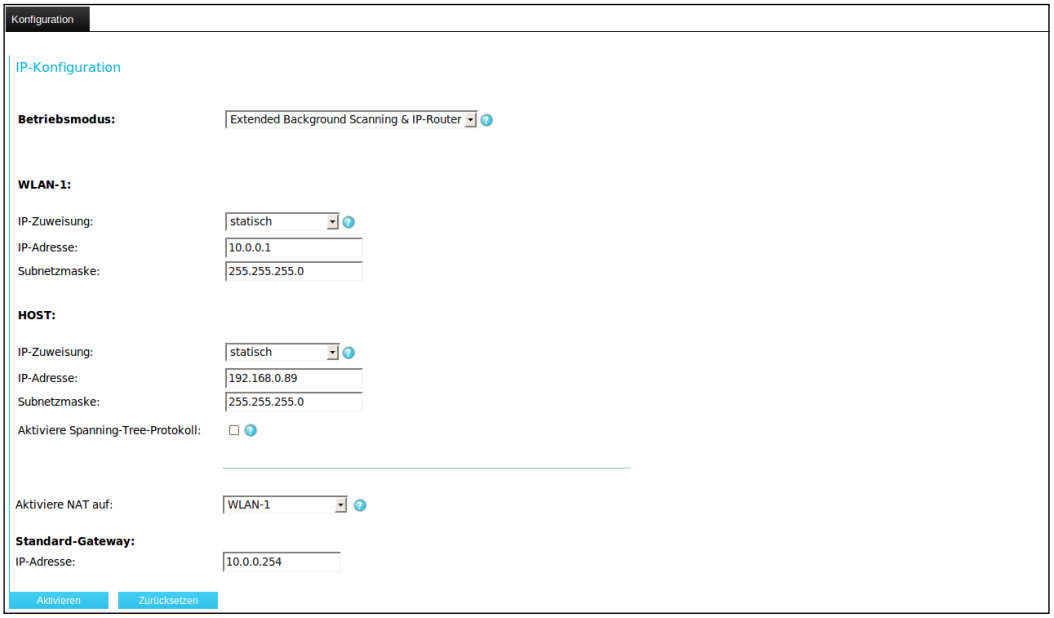
EXTENDED BACKROUND SCANNING (RAC112X)



Der RAC112x unterstützt jetzt den Betriebsmodus Extended Background Scanning. In diesem Betriebsmodus wird das WLAN2 Interface ausschließlich zum permanenten Scannen nach neuen AccessPoints verwendet. Sobald ein besserer AccessPoint gefunden wird bucht sich das WLAN1 Interface auf dem neuem AP ein. Alle Parameter für WLAN2 sind in diesem Modus deaktiviert.

Dieser Modus eignet sich besonders für schnelles Roaming im Zusammenspiel mit AccessPoint anderer Hersteller. Insbesondere ist der MultiClientBridge Modus mit dem Extended Background Scanning kombinierbar.

EXTENDED BACKROUND SCANNING & IP-ROUTER (RAC112X)



In diesem Modus können WLAN-1 und HOST mit eigenen IP-Adressen belegt werden. Die Schnittstelle WLAN-2 arbeitet automatisch als Background Scanning Schnittstelle.

Hinweis:

Der Betriebsmodus ist explizit für WHOST-Infrastrukturen mit Access Points die nicht von ads-tec sind und insbesondere für Setups mit Switched WLAN oder WLAN Controller.

8.3.2 WLAN-1 PARAMETER

Über das Menü Schnittstellen können die Schnittstellen des Access Points eingestellt werden. Jede Schnittstelle verfügt über eigene Einstellmöglichkeiten welche die Arbeitsweise der Schnittstelle beeinflussen. Außerdem können nicht verwendete Schnittstellen deaktiviert werden.

Hinweis:

Je nach Ausstattungsoption des Geräts können 2 WLAN Schnittstellen zur Verfügung stehen.

WLAN1 (ACCESS POINT) 2.4GHZ-802.11B/G:

Um Änderungen bzw. Einstellungen auf der Schnittstelle tätigen zu können, muss der Haken bei Aktiviere Schnittstelle gesetzt werden.

Betriebsmodus: Umschaltung / Auswahl: Access Point / Client (Diese Option ist nicht Verfügbar auf einem RAC111x oder RAC151x.

Verstecke SSID: Bei aktivierter Funktion wird die SSID (Netzwerkname) nicht angezeigt.

Netzwerkname (SSID): Name des Netzwerks. Default-Einstellung: **ads.** Die SSID kann maximal 32 Zeichen lang sein.

Hinweis:

Gültige Zeichen sind: a-z, A-Z, 0-9, Sonderzeichen: . _ - ? $ @ ! { } [ ] ( ) + # ; , < > | : * ~ % $ & / =

WLAN-Modus: Auswahl eines speziellen WLAN Modus

Kanal: Bietet die Möglichkeit einen speziellen Kanal oder die automatische Kanalsuche auszuwählen.

Hinweis:

Bei aktivem **Intelligent Channel Selection (ICS)** bilden alle ads-tec Access Points in einem lokalen Ethernet Segment einen Verbund und optimieren ihre Kanalauswahl anhand von verschiedenen Parametern. Dabei werden sowohl die Signalausbreitungsverhältnisse zwischen den Geräten erfasst und gemessen sowie auch andere störende Access Points ausserhalb des Netzwerkes berücksichtigt. Ein ads-tec Access Point startet die ICS Messung während des Bootvorgangs, wenn die Option erstmalig aktiviert wird oder wenn der **Remeasure Timer** abgelaufen ist. (Sichtbar durch abwechselnd blinkende (rot/grün) LEDs am HOST Port). Die Messphase benötigt ~100 Sekunden.Während dieser Zeit können sich keine WLAN Clients an dem AP anmelden. Wenn 5Ghz mit DFS konfiguriert wird verlängert sich die Zeit bis zur Bereitschaft auf ~160 Sekunden.

Übertragungsrate: Manuelles oder automatisches Einstellen der Mbit-Rate.

CTS/RTS Threshold: Ab dem hier eingestellten Wert wird dem Access Point ein Signal übermittelt, wenn ein Paket welches über der hier eingestellten Größe übermittelt werden soll. Der Access Point hält den Kanal für dieses Paket frei.

Fragmentation-Thresold: Sollte ein Paket den hier eingetragenen Wert überschreiten, dann wird das Paket fragmentiert und in kleinere Paket-Einheiten aufgeteilt.

Hinweis:

Diese Fragmentation-Thresold Funktion kann bei eingeschalteten WPA-Verschlüsselungsstandards nicht verwendet werden.

Langstrecken:
Wenn eine große Entfernung zwischen 2 Geräten zurückgelegt werden soll, kann hier der Timeout über die Angabe der Entfernung vergrößert werden. Der vergrößerte Timeout hat zur Folge, dass der Access Point eine längere Zeitspanne wartet um die Antwort der Gegenstelle besser entgegenzunehmen.

Sendeantenne:

Über die Auswahl der Sendeantenne kann eingestellt werden ob die Sendeantenne automatisch gewählt werden soll oder ob sie manuell eingerichtet werden soll.

Antennenverstärkung: Die Antennenverstärkung kann verwendet werden um eine höhere Sendeleistung zu erzielen. Außerdem sie durch die jeweils gültigen Bestimmungen des Landes begrenzt.

Beispiel: Eine Antenne mit dem Wert 10dbi und Kabel mit dem Wert 3db werden verwendet. er einzutragende Wert der Antennen-Verstärkung beträgt hier 7dbi.

Leistungsbeschränkung:

Die Leistungsbeschränkung limitiert de Access Point auf den angegeben Wert. Der hier eingetragene Wert wird auf alle Clients die Zugriff auf den Access Point haben übertragen.

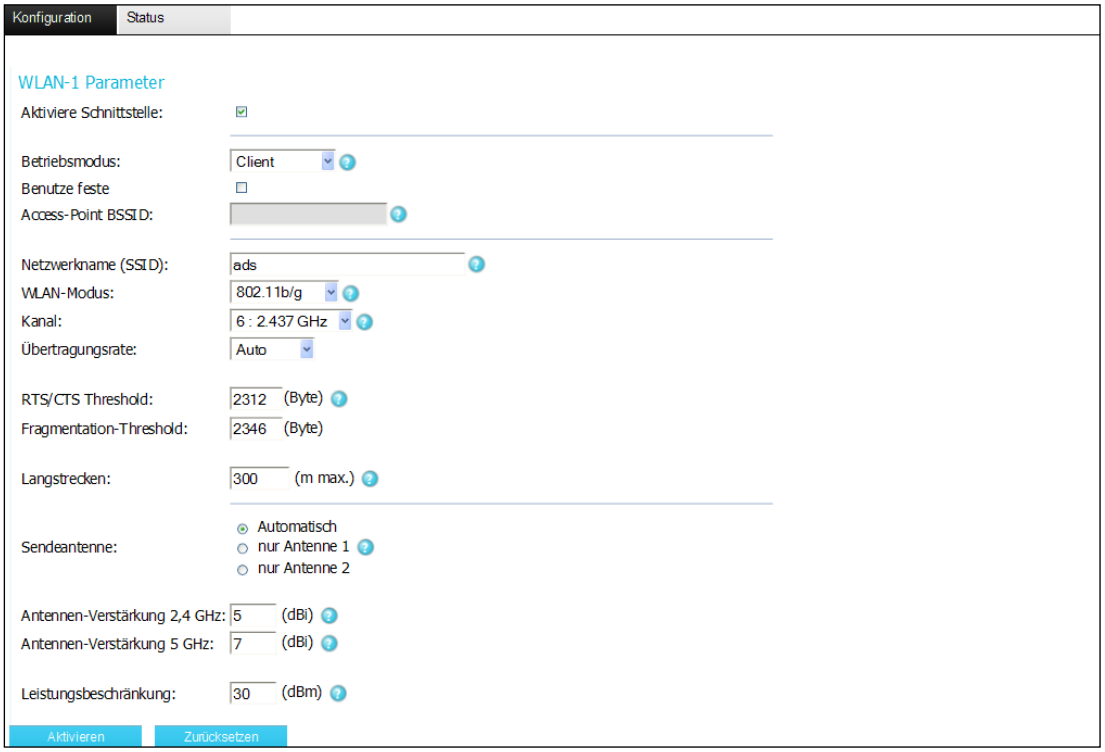
STATUS

Ansicht: Access Point

Die Statusanzeige der WLAN-1 Schnittstelle zeigt das Verhalten des Datenverkehrs an. Die Anzeige kann über **Aktualisieren** auf den neuesten Stand gebracht werden.

WLAN-1 (ACCESS CLIENT) 2.4 GHZ – 802.11B/G:

Die Auswahl Client unterscheidet sich lediglich in den Punkten der nun fehlenden Option „Hide SSID“ und der neuen Option: „feste BSSID“:



Benutze feste Access Point BSSID:

Wenn die Option aktiviert ist, kann die MAC-Adresse eines Access Points eingetragen werden. Diese Option ist bei Access Points mit identischer SSID hilfreich, weil genau das jeweilige Gerät angesteuert werden kann.

Bestätigen Sie anschließend mit **Aktivieren.**

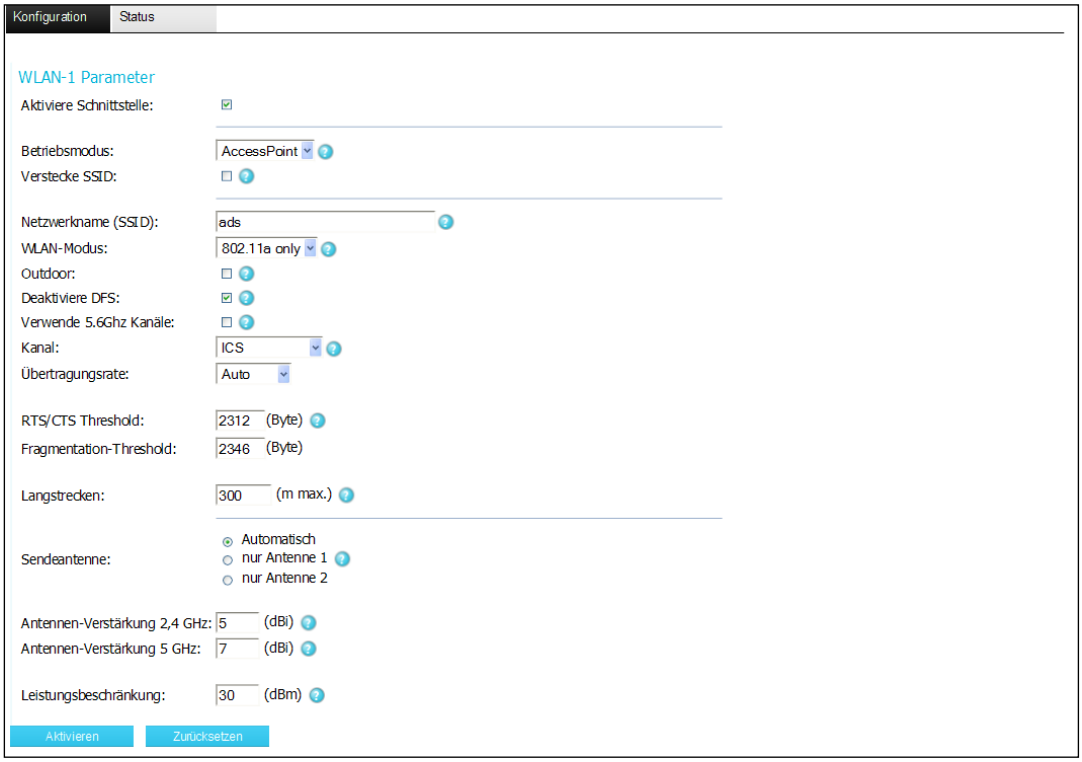
STATUS

Ansicht Access Client:

Die Statusanzeige der WLAN-1 Schnittstelle zeigt das Verhalten des Datenverkehrs an. Die Anzeige kann über **Aktualisieren** auf den neuesten Stand gebracht werden.

WLAN1 (ACCESS POINT & ACCESS CLIENT) 5 GHZ – 802.11A (ETSI):

Wird der WLAN-Modus 802.11a (Access Point) oder 802.11a/b/g (Access Client) konfiguriert, dann ändern sich einige verfügbare Optionen:



Hinweis:

Die Option „Outdoor“ ist nur im Access Point Modus verfügbar. Die Option Deaktiviere DFS steht in beiden Modi zur Verfügung.

Indoor/Outdoor:

Muss aktiviert werden, falls der Access Point Teil einer Funkverbindung im Freien ist. Bestimmte Kanäle des 5GHz Bandes dürfen nicht im Freien verwendet werden, diese werden mit dieser Option ausgeschlossen. Bei Verwendung nur im Innenbereich kann die Option Indoor verwendet werden. Bei Access Clients spielt diese Option keine Rolle.

Deaktivere DFS:

Wird der Access Point NICHT im Freien betrieben darf DSF deaktivert werden. Die Kanäle 36,40,44 und 48 dürfen dann auch von Hand fest eingestellt werden. Zusätzlich wird die maximal zulässige Abstrahlleistung reduziert. Im Client Betriebsmodus dagegen darf DFS auch im Freien deaktivert werden.

Verwende 5.6 Ghz Kanäle:

Es werden die Kanäle 120,124 und 128 aktiviert. Bei aktivierter DFS-Funktion muss eine Ansprechzeit (Channel Availability Check Time) von 10 Minuten eingehalten werden.

Hinweis:

Im Client Modus ist die DFS Funktion Standardmäßig deaktivert. Durch die Radar-Erkennung während der Datenübertragung kann es insbesondere beim Client zu starken Interferenzen kommen welche dann als Mögliche Radar Impulse ausgewertet müssen. Eine sehr hohe CPU Last und fehlerhafte häufige Radar-Detektionen sind die Folge. DFS sollte daher im Client Modus nur aktiviert werden wenn die höhere Abstrahlleistung des Client von 23dB überschritten wird und 30dBm nötig sind um eine stabile Datenverbindung zu erreichen. Befindet sich in unmittelbarer Nähe ein weiteres 5 GHz Gerät kann dies ebenfalls zu erheblichen Störungen des Client-Modus führen wenn DFS aktiv ist.

WLAN1 (Access Point & Access Client) 2.4 GHz – 802.11a (FCC):

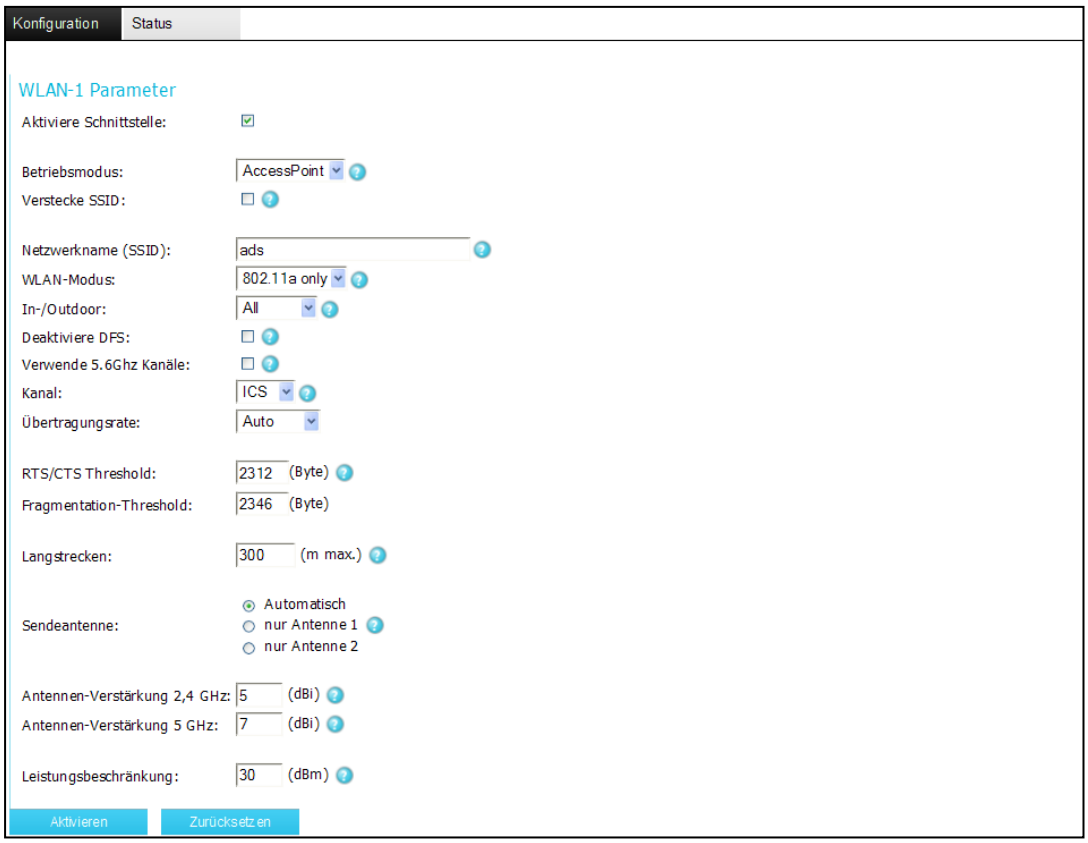
Die FCC Version der Schnittstelleneinstellungen haben folgende zusätzliche Einstellungmöglichkeiten:

Outdoor:
Diese Funktion muss aktiviert sein, wenn das Gerät im Freien eingesetzt wird. Die Funktion deaktiviert die Kanäle, die nicht im Außeneinsatz verwendet werden dürfen.

Richtfunkantenne: Sollte eine Richtfunkantenne angeschlossen sein, muss die Checkbox aktiviert werden.

Hinweis:

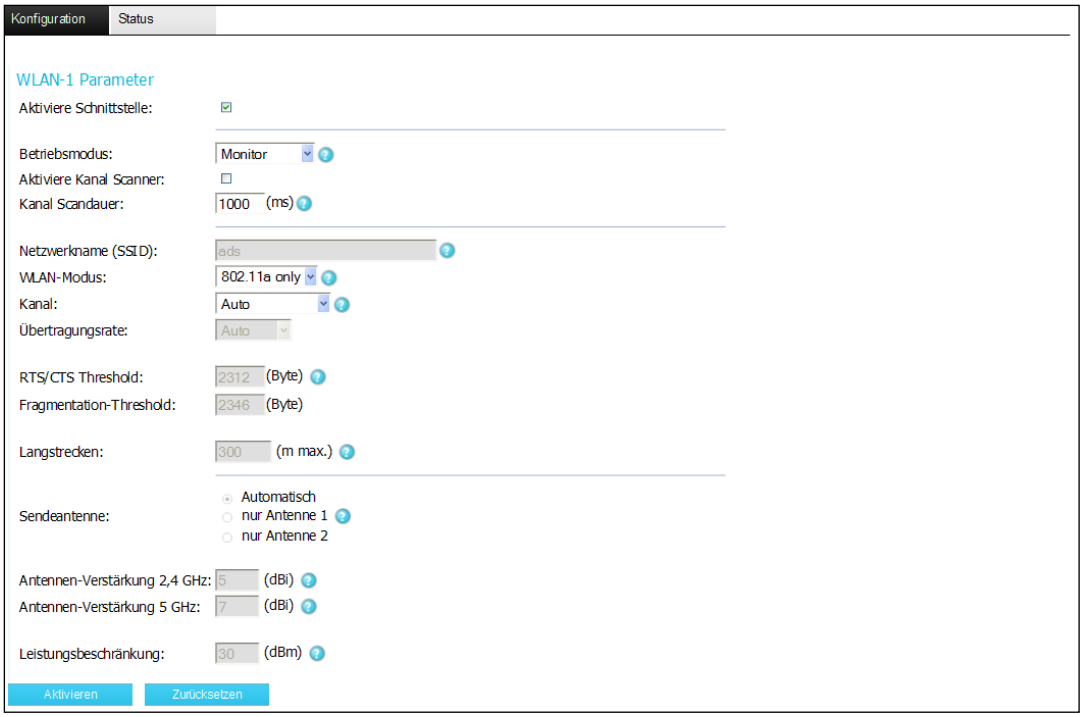
DFS und TPC sind hier deaktiviert. Die Version 802.11b/g (FCC) hat im Gegensatz zur A-Version nur zusätzlich noch die Richtfunkantennen-Einstellung.



MONITOR

Im Monitor Modus können Datenpakete aufgezeichnet und an einen PC übertragen werden.

Hinweis:
Diese Funktion ist nur in Kombination mit Remote Capture funktionsfähig.



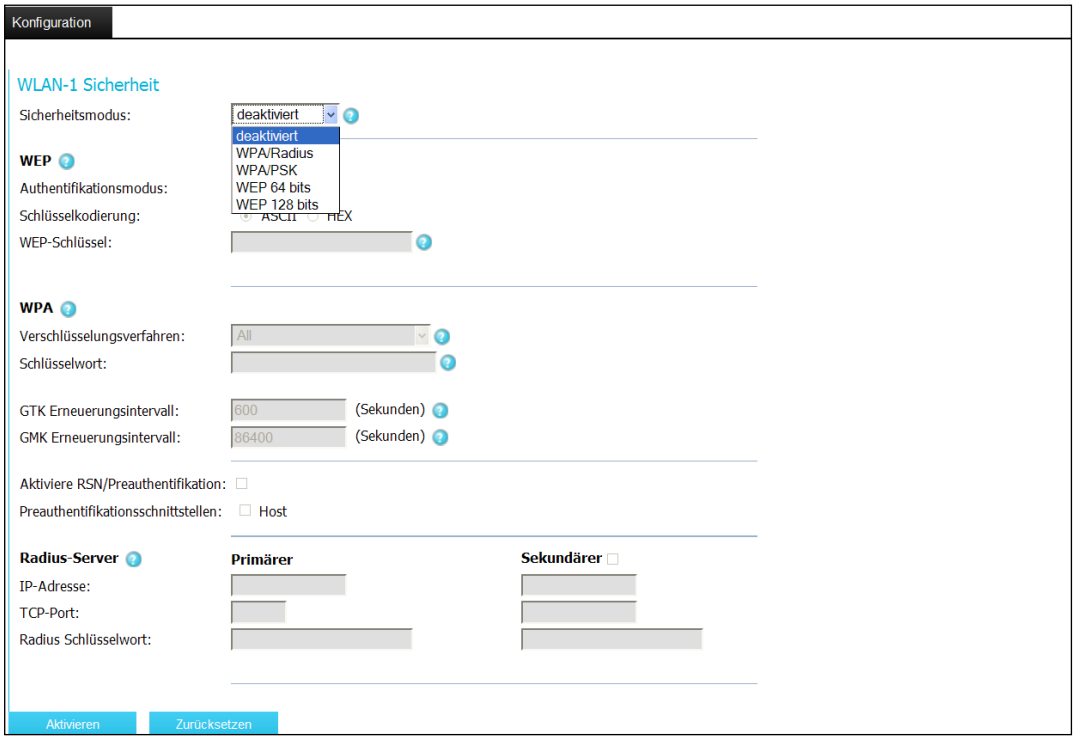
Aktiviere Kanal Scanner:

Bei aktivierter Funktion werden alle verfügbaren Kanäle nacheinander durchlaufen und für die eingestellte Dauer Pakete mitgeschnitten.

8.3.3 WLAN-1 SICHERHEIT

WLAN 1 / 2

Die WLAN Sicherheit ermöglicht die Konfiguration des entsprechenden Sicherheitsstandards für das WLAN-Netzwerk. Zur Auswahl stehen folgende Modi:

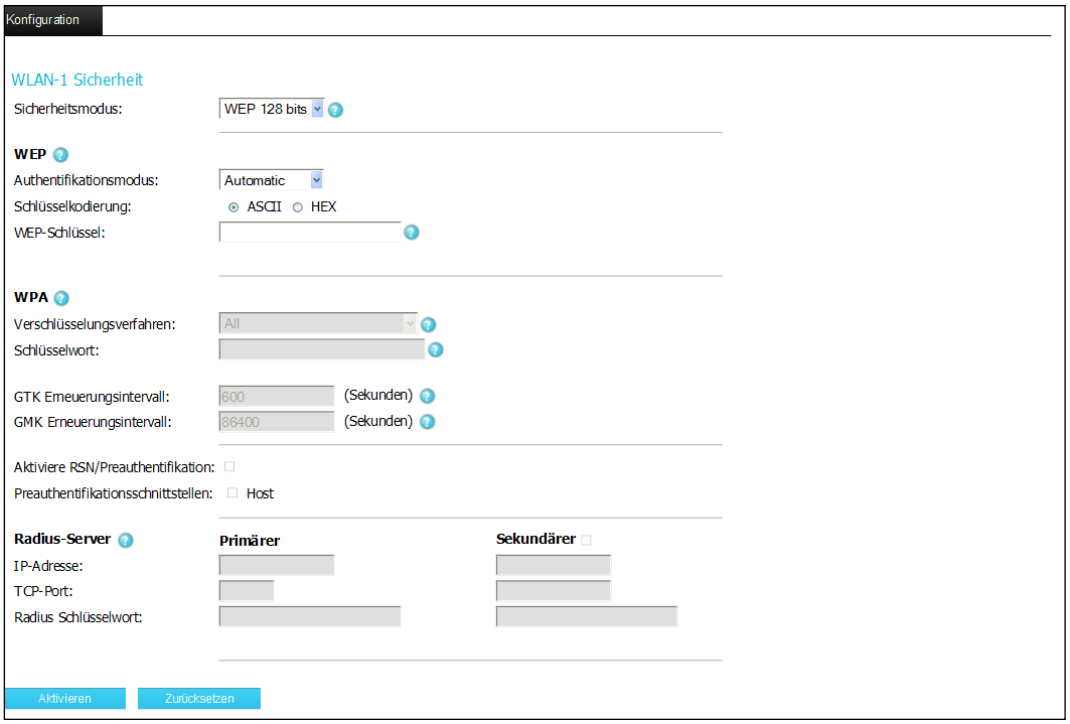


WEP 64 Bits / WEP 128 Bits

Hinweis:

Der WLAN-Modus 802.11n ist nicht kompatibel mit den Sicherheitsstandards WEP und WPA1. Bei Verwendung dieser Sicherheitsstandards fällt der WLAN-Modus automatisch auf 802.11g bzw. 802.11a zurück.

Bei WEP 64 Bits / 128 Bits Modus wird wie bei WPA ein Schlüsselwort verwendet, welches den Zugang zum WLAN-Netzwerk regelt. Der Unterschied besteht darin das im WEP-Modus der Schlüssel nicht verändert wird, sondern statisch bleibt.



Authentifikationsmodus:

Automatic:

Der Modus Automatic wählt den Authetifikationsmodus selbständig.

Open System:

Die **Open System** Authentication ist die Standard-Authentifizierung.

Shared Key:

Die Shared Key Authentication verwendet einen erweiterten Handshake Mechanismus beim Einbuchungsvorgang, der jedoch keine weitere Sicherheit bringt.

Schlüsselkodierung:

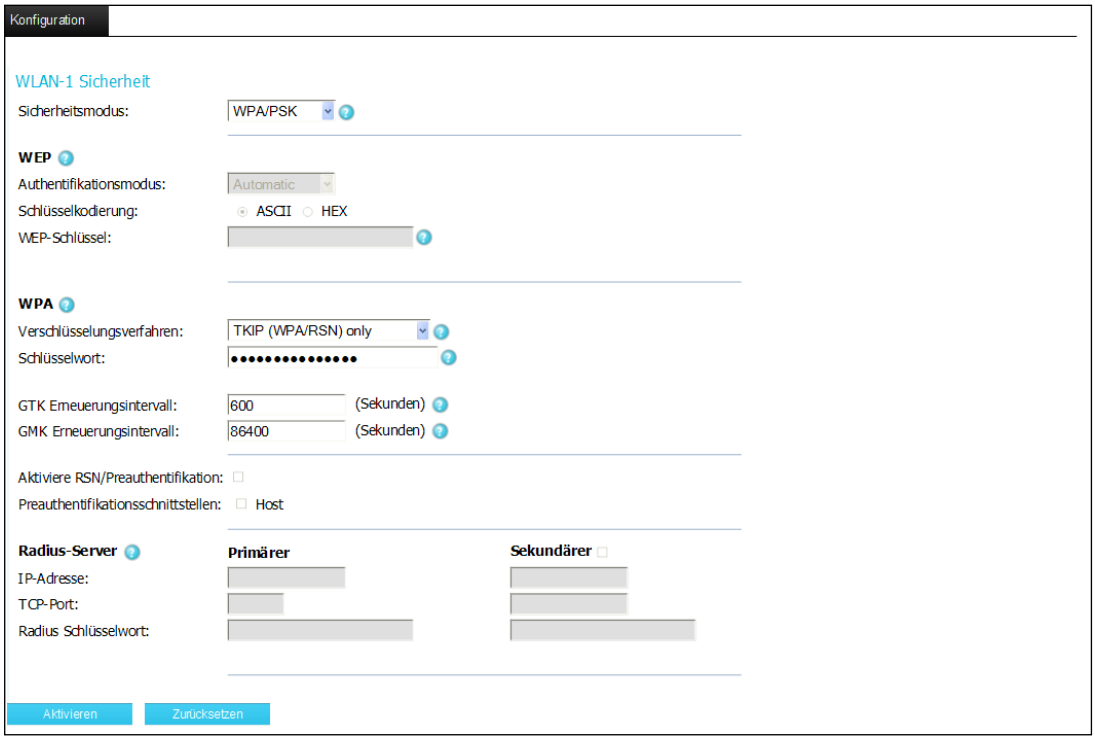
Wahlweise kann eine Schlüsselkodierung ASCII oder HEX verwendet werden. ASCII ist eine 7-Bit Kodierung, HEX verwendet eine 16-Bit Kodierung.

WEP-Schlüssel:

Der WEP-Schlüssel ist bei ASCII-Wahl auf 5 Zeichen begrenzt. HEX ermöglicht die Eingabe eines 10 stelligen WEP-Schlüssels. Bei der Wahl des Schlüssels sollten keine Wörter, sondern Buchstaben und Zahlenkombinationen verwendet werden.

WPA/PSK

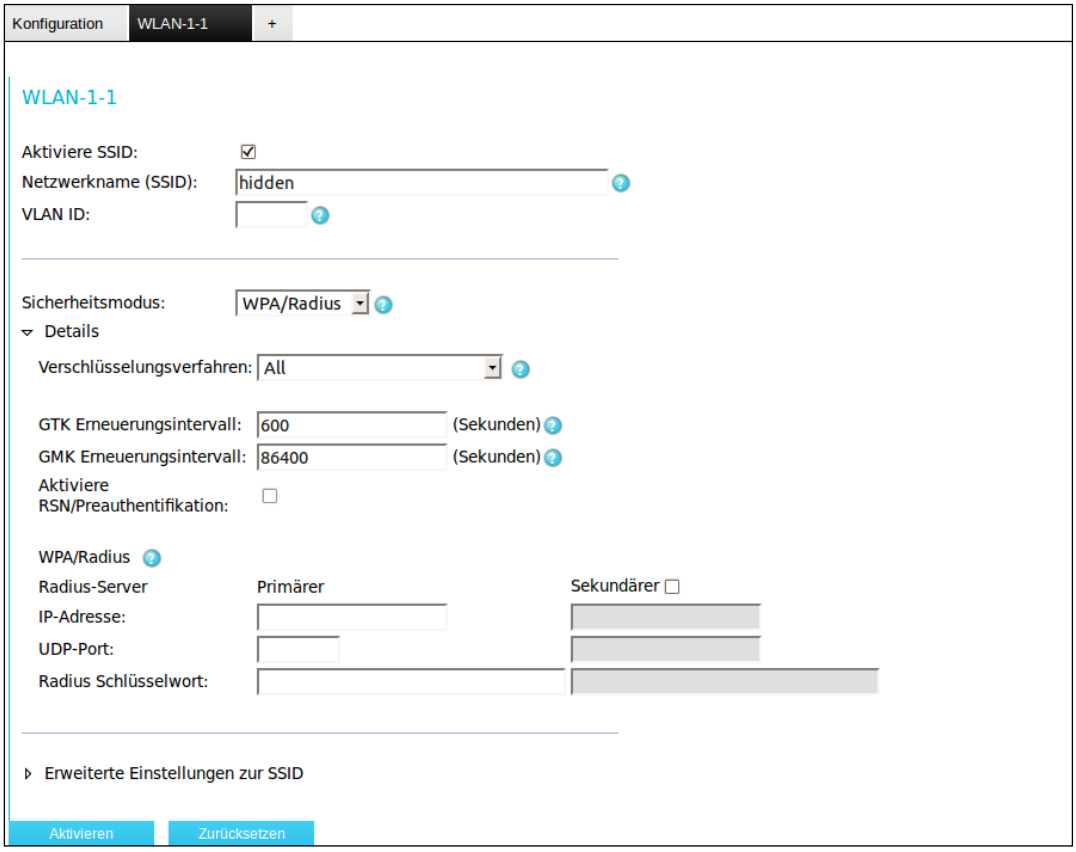
Im WPA/PSK Modus wird ein Schlüsselwort in Kombination mit einem speziellen Verschlüsselungsverfahren verwendet. Das Schlüsselwort (Pre shared key) darf minimal 8 und maximal 63 Zeichen enthalten. Es wird empfohlen keine Wörter sondern Kombinationen aus Buchstaben, Zahlen zu verwenden, um die Sicherheit optimal zu gewährleisten.



Verschlüsselungsverfahren:

Es besteht die Möglichkeit alle Verschlüsselungsverfahren oder ein spezielles Verschlüsselungsverfahren zu verwenden. Hierbei ist zu beachten, dass der Standard WPA 2 von allen Geräten unterstützt werden muss, um eine Funktionalität zu gewährleisten.

WPA RADIUS



Der Access Point ist in der Lage einen vorhandenen RADIUS-Server für die Authentifizierung des Acounts zu verwenden. Dazu muss die IP-Adresse des Radius-Servers im Feld IP-Adresse eingetragen werden.

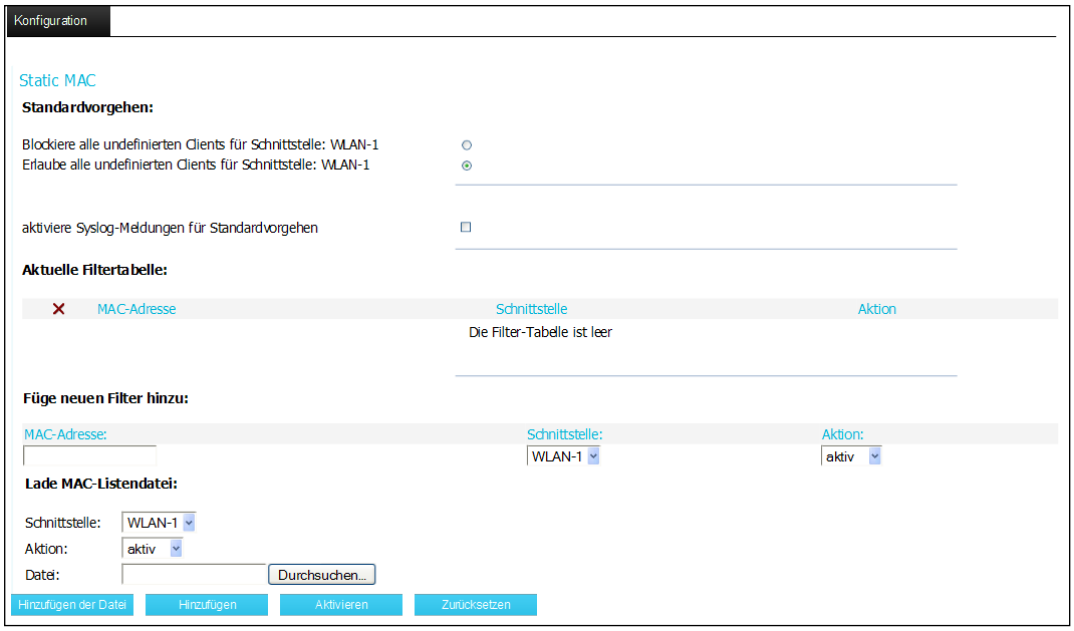
Der UDP-Port auf welchem der RADIUS-Server betrieben wird muss ebenfalls unter UDP-Port eingetragen werden. In der Regel läuft der Radius Server auf UDP Port 1812.

Über das RADIUS-Schlüsselwort wird der Access Point am RADIUS-Server identifiziert und authentifiziert.

Wenn zwei RADIUS-Server verwendet werden kann alternativ eine andere Konfiguration unter Sekundär eingetragen werden. Diese Angaben treten nur dann in Kraft wenn der Primäre RADIUS-Server nicht erreicht werden konnte. Der Access Point versucht dann eine Verbindung zum Sekundären RADIUS-Server herzustellen. Bestätigen Sie mit Aktivieren.

8.3.4 STATISCHE MAC-ADRESSE

Der statische MAC-Filter kann verwendet werden um eine Schnittstelle welche als Access-Point konfiguriert ist mit einer Zugangskontrolle zu versehen. Dabei wird die MAC-Adresse eines WLAN-Clients gegen die konfigurierte Zugangsliste geprüft und ein Zugang gewährt. Ist der Zugang für einen Client gesperrt wird er bei einem 802.11 Einbuchungsvorgang abgewiesen. Da eine MAC Adresse leicht zu fälschen ist bietet diese Konfiguration keine sehr hohe Sicherheit. Bei einer WPA-Verschlüsselung ist sie nicht sinnvoll da WPA selbst bereits ausreichende Sicherheit gewährt. Lediglich bei einer WEP-Verschlüsselung kann ein MAC-Filter als Zusatz-Schutz sinnvoll sein. Ist eine Schnittstelle nicht im Access-Point Modus kann die Filtertabelle nicht verwendet werden. Der Text: „Keine WLAN-Schnittstellen im AP-Modus. Filter ist inaktiv“ erscheint. Den Menüpunkt gibt es nicht bei einem RAC111x oder RAC151x.



Standardvorgehen:

Das Standardvorgehen definiert was mit einer MAC-Adresse in der Filtertabelle passieren soll. Ein Client kann entweder explizit ausgesperrt werden (Blacklist) oder zugelassen werden (Whitelist). Letzteres ist die in den Meisten Fällen verwendete Einstellung.

Syslog:

Ist diese Option gesetzt wird eine Meldung im Eventlog generiert wenn ein Client abgewiesen wird weil er explizit ausgesperrt ist oder nicht zugelassen wird.

Neuer Filter:

Um einen neuen Filter-Tabellen Eintrag anzulegen muss die MAC Adresse des Clients im Format z.B. 00:50:C2:48:A1:BB angegeben werden sowie die Schnittstellen auf denen der Eintrag gültig sein soll. (WLAN-1, WLAN-2, *) . Unter „Aktion“ kann „aktiv“ oder „inaktiv“ gewählt werden um einen einzelnen Eintrag vorübergehend abzuschalten bzw. nicht sofort zu aktivieren. Danach muss auf „**Hinzufügen**“ geklickt werden.

MAC-Listendatei:

Sollen mehrere MAC-Adressen auf einmal konfiguriert werden ist es Hilfreich eine Textdatei mit einer Liste aller MAC-Adressen zu verwenden. Der Inhalt einer solchen Datei enthält eine MAC-Adresse pro Zeile, z.B.

00:50:C2:48:A1:00

00:50:C2:48:A1:02

00:50:C2:48:A1:01

Zusätzlich muss ausgewählt werden ob alle so geladenen MAC-Adressen „**aktiv**“ oder „**inaktiv**“ sein sollen und auf welcher Schnittstelle sie gelten sollen. Die Liste wird den bereits vorhandenen Einträgen hinzugefügt. Maximal können 500 Einträge gespeichert werden.

Hinweis:

Bei einer langen Liste kann die Verarbeitung sehr lange dauern, pro Eintrag wird ca 1 Sekunde benötigt. Diese Zeit wird danach auch beim Booten benötigt wenn die Einstellungen geladen werden.

8.3.5 PAKETFILTER

Hinweis:

Der Paketfilter kann genauso über die Startseite des Webinterfaces gestartet werden.

Der Paketfilter unterstützt beim Erstellen von Regeln in dem eine schrittweise Benutzerführung die häufigsten Konfigurationsparameter einer Regel automatisch abfragt.

Hinweis:

→Die Regeln werden entsprechend ihrer Reihenfolge beginnend mit dem ersten Regelset durchlaufen.

→Ein Regelset wird für ein Paket nur beachtet wenn die Einstellung "ein-/ausgehende" Schnittstelle mit dem Paket übereinstimmt.

→Wird ein Regelset durchlaufen, so werden die darin befindlichen Regeln von oben nach unten durchlaufen.

→Sobald eine Regel in einem durchlaufenen Regelset genau auf das Paket passt, wird die zugehörige Aktion ausgeführt und keine weitere Regel geprüft.

Jedes Ruleset kann bis zu 10 Regeln enthalten, wobei alle Regeln eines Rulesets die gleiche Einstellung bezüglich der betroffenen eingehenden und ausgehenden Schnittstelle haben. Auf der Hauptseite des Paketfilters werden die aktiven Layer 2 -Rulesets angezeigt.

Durch eine Filter-Funktion am Seitenende können die angezeigten Rulesets anhand der eingehenden und ausgehenden Schnittstellen eingeschränkt werden. Dies hat keinen Einfluss auf die Funktionalität der Regeln: nicht angezeigte Regeln sind trotzdem aktiv.

Über der Filter-Funktion für ein- und ausgehende Schnittstellen befindet sich die Symbolleiste um neue Rulesets hinzuzufügen. Durch einen Klick auf das Plus-Symbol erscheint ein Dialog, der den Benutzer Schritt für Schritt durch die Einstellungsmöglichkeiten der verschiedenen Protokoll-Ebenen führt.

Im Betriebsmodus IP-Router erweitert mit ausgewählter Layer 2 Ebene können nur Open VPN Schnittstellen gefiltert werden. Die Layer 3 Ebene ermöglicht die Filterung aller Schnittstellen in belieber Richtung, die über eine IP-Adresse verfügen, in beliebiger Richtung.

Es erscheinen in der Liste nur die Regelsets für welche die eingehende und ausgehende Schnittstellen sowie die Kommunikationsrichtung übereinstimmen.

Hinweis:
Nach Definition der Regeln ist zur Funktionsprüfung in der Weboberfläche **Änderungen anwenden** auszuwählen.

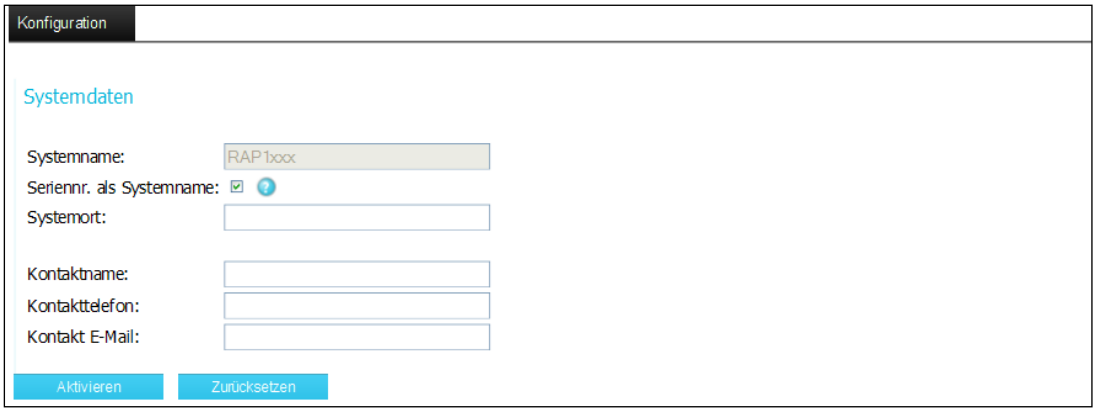
8.3.6 GRUNDEINSTELLUNGEN

SYSTEMDATEN

Über das Bedienfeld Systeminformationen können wichtige Informationen wie Ort und Service-Adressen hinterlegt werden. Diese Informationen dienen der eindeutigen Identifikation des Geräts an seinem Standort und den zugehörigen Kontaktdaten, die im Servicefall hier eingesehen werden können.

Seriennr. als Systemname:

Diese Option ist standardmäßig aktiviert und zeigt den Systemname und die Seriennummer des Geräts an.



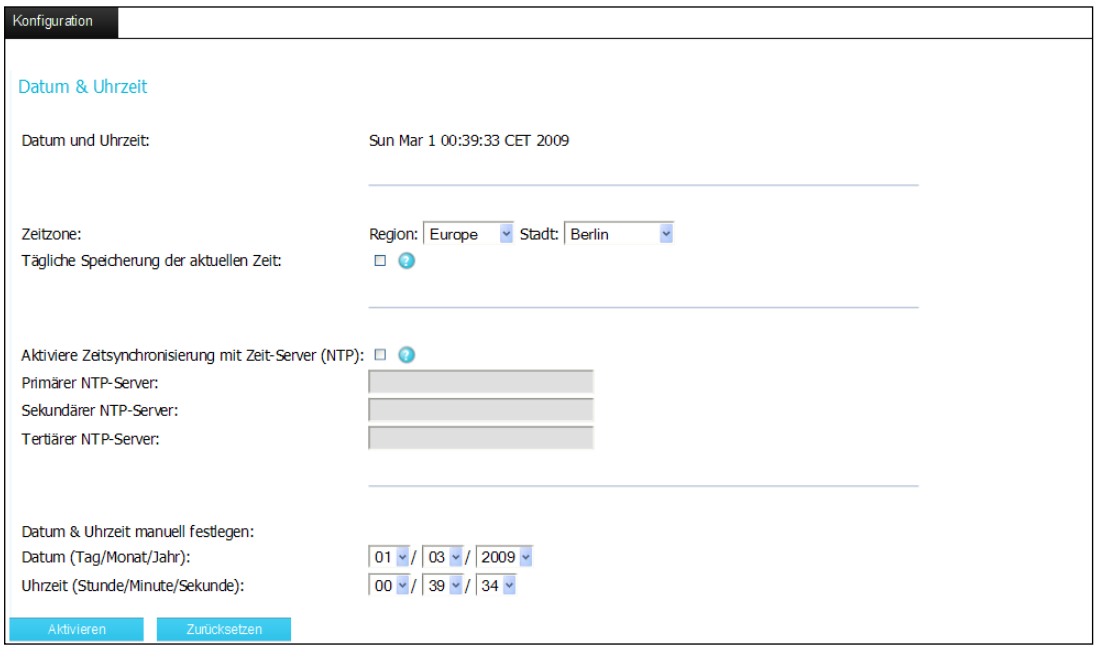
Um ihre getätigten Einstellungen zu übernehmen klicken Sie auf **Aktivieren.**

DATUM & UHRZEIT

Über **Datum & Uhrzeit** kann die Konfiguration des Datums und der Uhrzeit vorgenommen werden.

Das Gerät verfügt nicht über eine Real Time Clock. Daher fallen die Einstellungen nach einem Spannungsausfall auf die zuletzt gespeicherten Einstellungen zurück..

Über die Aktivierung und Eingabe der IP-Adresse des NTP-Servers wird die Uhrzeit automatisch synchronisiert.



Zeitzone:

Das Drop-Down-Menü ermöglicht das Einstellen der korrekten Zeitzone.

Tägliche Speicherung der aktuellen Zeit:

Bei angehakter Option wird die aktuelle Systemzeit gespeichert.

Aktiviere Zeitsynchronisierung mit Zeit-Server (NTP):

Die Funktion ermöglicht das Synchronisieren von Datum & Uhrzeit über drei verschiedene NTP-Server. Sobald ein NTP-Server erfolgreich antwortet wird dieser verwendet.

Aktivieren Sie dazu die Checkbox neben der Option und tragen Sie die IP-Adresse des NTP-Servers ein.

Datum & Uhrzeit manuell festlegen:

Hier kann das aktuelle Datum und die Uhrzeit manuell eingestellt werden.

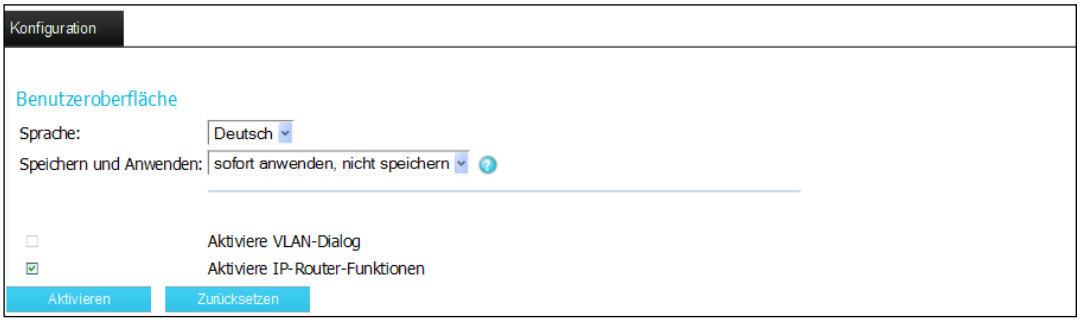
Um Ihre Änderungen zu übernehmen klicken Sie auf **Aktivieren.**

Hinweis:

Die Datum- und Uhrzeiteinstellung ist für das Erstellen von Zertifikaten, Auswerten von Eventlog-Einträgen und die zeitbasierten Regeln wichtig. Ohne aktivierten NTP-Server geht die aktuelle Zeit nach einem Spannungsabfall verloren und muss manuell neu eingestellt werden.

BENUTZEROBERFLÄCHE

Im Menü „**Benutzeroberfläche**“ besteht die Möglichkeit, die Sprache des Web-Interfaces auf deutsch oder auf englisch zu stellen.



Im Drop Down Menü lassen sich die Optionen „**sofort Anwenden & nicht speichern**“ und „**nicht anwenden & nur speichern**“ auswählen.

Die Funktion „**Sofort Anwenden & nicht speichern**“ zeigt auf allen Seiten im Access Point Menü einen „Anwenden“ Button mit dem getätigte Änderungen sofort angewandt werden können. Um die Neue Konfiguration auch nach einem Neustart beizubehalten, müssen die Einstellungen per Klick auf dem nun blinkenden Diskettensymbol gesichert werden.

Die Funktion „**nicht Anwenden & nur Speichern**“ zeigt einen „Speichern Button auf allen Seiten im Access Point Menü. Geänderte Einstellungen werden nicht angewandt, dafür aber sofort gespeichert.

Der “**Bitte warten**“ Dialog, der beim Absenden einer Seite angezeigt wird, entfällt. Anstatt des Diskettensymbols blinkt nun ein Neustart Symbol, welches zur Startseite führt wo ein Neustart durchgeführt werden kann.

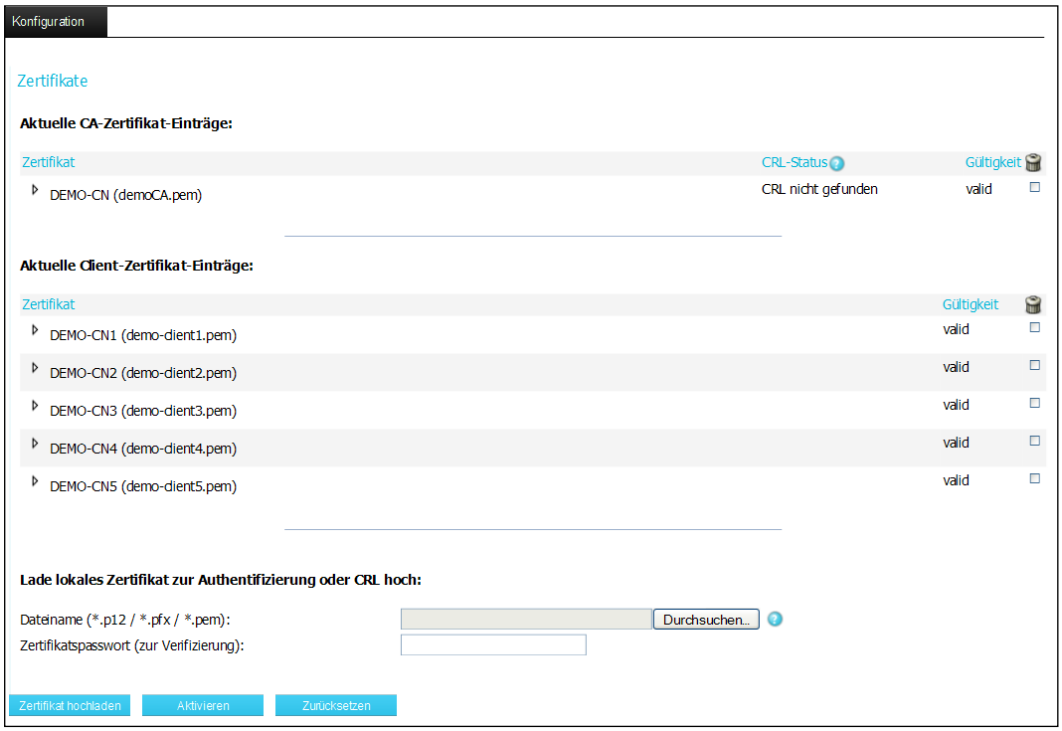
Ausnahmen bei denen der „**Bitte warten**“ Screen angezeigt wird sind spezielle Aktionen wie Ping Test und Firmware-Updates.

Bestätigen Sie ihre Einstellungen mit **Aktivieren**.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

ZERTIFIKATE

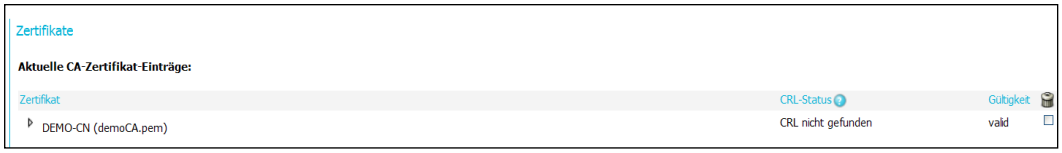
Die Zertifikate dienen im Access Point zur Authentifizierung bei L2TP/IPSec, OpenVPN und dem HTTPS- Webserver. In dieser Webseite der Zertifikatsverwaltung des Access Points sind bereits einige Demozertifikate angelegt die nur zu Testzwecken dienen.



Wird ein Zertifikat hochgeladen, so wird dessen Gültigkeit automatisch überprüft. Ein ungültiges Zertifikat, bei dem z.B. der Zeit- & Datumsbereich nicht mit der Systemzeit des Access Points übereinstimmen, wird in der Gültigkeitsspalte als invalid angezeigt. Daraufhin erscheint zum ungültigen Zertifikat ein Fragezeichensymbol über das weitere Informationen zur Systemfehlermeldung in englischer Sprache abgerufen werden kann.

CRL-ZERTIFIKATE:

Der CRL Status eines Zertifikates wird in der obigen Zeile angezeigt.



Einzelne Zertifikate können als invalid erscheinen wenn ein Zertifikat mittes CRL zurückgezogen wurde.

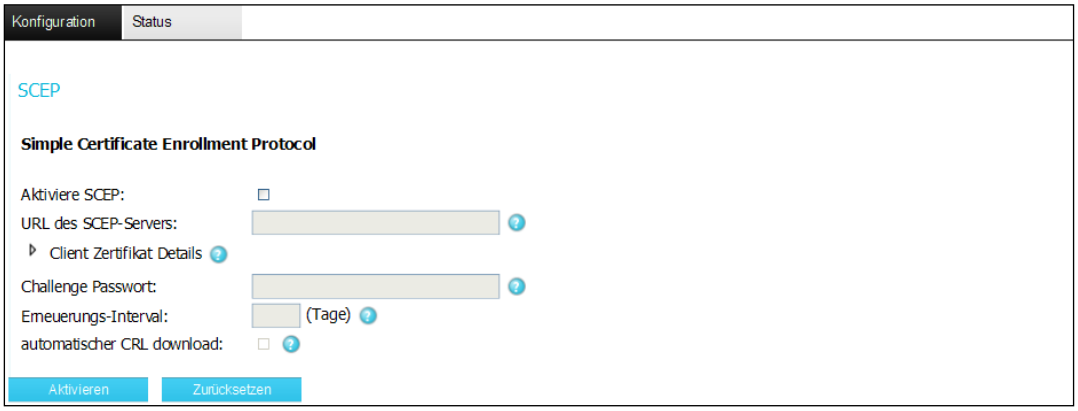
Hinweis:

Eine Client-Zertifikatsdatei muss sowohl einen privaten Schlüssel als auch einen öffentlichen Zertifikatsanteil enthalten. Der private Schlüssel muss im RSA-Format vorliegen.

Um ihre Einstellungen zu übernehmen wählen Sie **Aktivieren**.

SCEP:

Ermöglicht die Verwendung eines SCEP Zertifikats Dienstes (z.B. Windows 2008 Server). Bei Verwendung der Funktion wird dem Gerät automatisch ein Zertifikat zugewiesen.



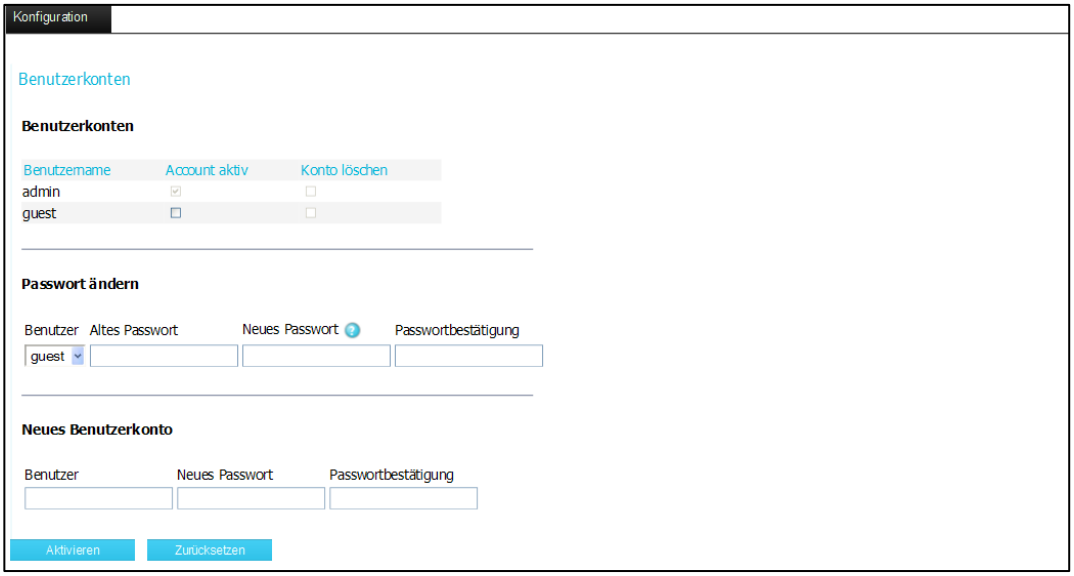
STATUS

Visualisiert den Zertifikatsupdatevorgang.

8.3.7 ZUGRIFFSRECHTE

BENUTZERKONTEN

Über Benutzerkonten können die Benutzer des Gerätes angelegt und in Ihren Rechten entsprechend konfiguriert werden.



Benutzerkonten

Listet die aktuell konfigurierten Benutzerkonten auf. Es besteht die Möglichkeit Benutzerkonten zu deaktivieren bzw. komplett zu löschen.

Durch die Aktivierung des Gast Accounts steht ein Benutzer zur Verfügung über den alle Konfigurationen des Geräts eingesehen, jedoch nicht verändert werden können.

Wenn der Gast Account aktiviert wird, ohne ein neues Passwort zu setzen, so wird das Passwort **guest** verwendet. Für das erstmalige setzen des Gast Passwortes ist als **altes Passwort** ebenfalls **guest** zu verwenden.

Passwort ändern

Über **Passwort ändern** kann das Passwort des jeweiligen Benutzerkontos geändert werden. Das hier definierte Passwort wird beim Aufruf der Weboberfläche vom Browser abgefragt. Um ein bereits vergebenes Passwort zu ändern, geben Sie das aktuelle Passwort in das Feld **Altes Passwort** ein. Wählen Sie ein neues Passwort und bestätigen Sie dieses erneut im Feld **Passwortbestätigung**.

Der vordefinierte Benutzer **admin**, der weder gelöscht noch aktiviert werden kann, darf als einziger Benutzer die Passworte anderer Benutzer ändern, ohne ein altes Passwort angeben zu müssen.

Neues Benutzerkonto

Ermöglicht die Erstellung eines neuen Benutzerkontos. Es ist ein Benutzername und ein Passwort zu definieren. Um das Konto zu erstellen klicken Sie auf **Aktivieren**.

Hinweis:

Der Menüpunkt Benutzerkonten dient lediglich der **Kontenverwaltung**. Die Zuweisung der Rechte für ein Benutzerkonto erfolgt über den Menüpunkt **Variablenrechte**.

Hinweis:

Ein neu angelegtes Benutzerkonto muss über die Checkbox „**Account aktiv**“ aktiviert werden.

Wechsel des Accounts:

Um zwischen Accounts zu wechseln kann der Link **User:xxxx** am Ende der Navigationsleiste verwendet werden. Geben Sie nun die erforderlichen Daten für den zu wechselnden Account ein. Anschließend ist der neue Account aktiviert.

Hinweis:

Um sich von der Weboberfläche abzumelden, kann der Link ebenfalls verwendet werden. Im darauffolgenden Dialogfenster muss dann mit **Cancel** bestätigt werden.

Hinweis:

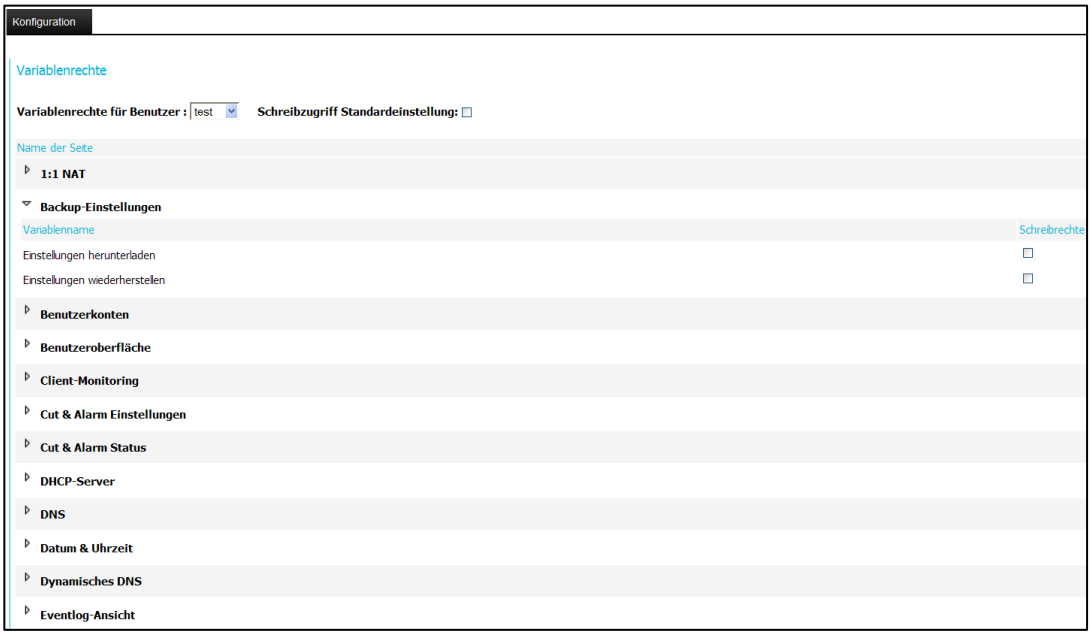
Das gewählte Passwort muss 4-20 Zeichen lang sein. Gültige Zeichen sind: 0-9, A-Z, a-z, sowie „-._# /@“.

Hinweis:

Falls Sie die browserspezifische Option “Kennwort speichern“ verwendet haben, kann es vorkommen das die Abmeldung über den Link nicht richtig funktioniert. Daktivieren Sie dann ggf. die Einstellung in ihrem Browser oder wählen Sie in ihrem Browser die entsprechende Option um aktive Authentifizierungen zu löschen.

VARIABLENRECHTE

Über Variablenrechte können neu angelegten Benutzerkonten entprechende Schreibrechte wie z.B. Schreibzugriff auf bestimmte Bereiche zugewiesen werden. Beispielhaft wurde das Benutzerkonto **test** erstellt, welches nun entsprechend konfiguriert werden soll.



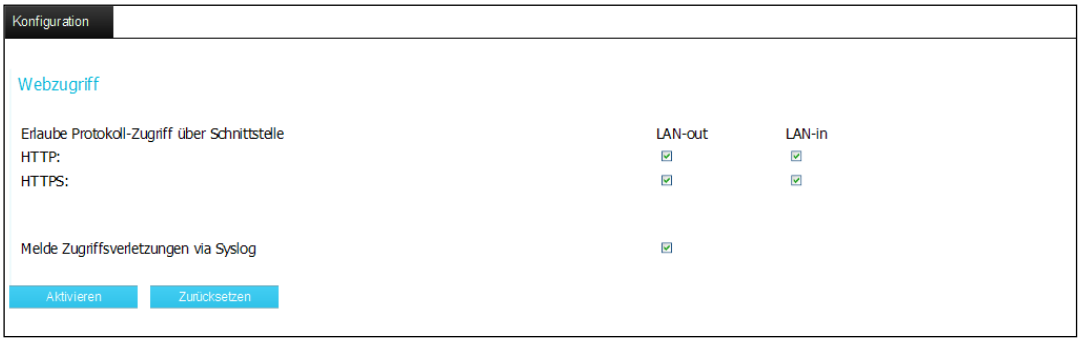
Jede Einstellung kann durch einmaliges Klicken geöffnet werden. Über die Checkbox an jeder Einstellung kann festgelegt werden, in welchen Bereichen Schreibrechte zugewiesen werden sollen.

Alle getätigten Einstellungen müssen mit **Aktivieren** bestätigt werden.

Um ein zusätzliches admin-Konto zu erstellen, welches die gleichen Eigenschaften wie das Default admin-Konto aufweist, kann die Checkbox „**Schreibzugriff-Standardeinstellung**“ gewählt werden. In einem Punkt unterscheidet sich dieses admin-Konto jedoch vom Benutzer „**admin**“: nur der Benutzer „**admin**“ darf Passwörter anderer Benutzer ändern, ohne das alte Passwort zu kennen. Wenn Sie die Option „**Schreibzugriff Standardeinstellung**“ nutzen, können Sie Außnahmen von diesen Schreibrechten einstellen, indem Sie bei einzelnen Variablenrechten die Schreibrechte über die Auswahlbox entfernen.

WEBZUGRIFF

Die **Webinterface-Zugriffskontrolle** erlaubt das Einstellen des Zugriffs über HTTP und HTTPS auf die – je nach Betriebsmodus verfügbaren HOST und HOST Schnittstelle. Außerdem kann eingestellt werden, ob Zugriffsverletzungen über den Eventlog gemeldet werden sollen.



(Ansicht Transparent Bridge)

Um einen Zugriff zu verweigern, muss der Haken bei der jeweiligen Option entfernt werden.

Bestätigen Sie ihre Änderungen mit **Aktivieren**.

8.3.8 ADV.WLAN

IAPP

IAPP dient dazu Steuerungs- und Zusatzinformationen zwischen Access-Point auszutauschen. So sendet z.B. ein AP einen IAPP-Notification an alle anderen APs im Netz wenn sich ein Client einbucht. Daraufhin können alle anderen APs den Client aus ihrer Tabelle der eingebuchten Clients entfernen. Die ebenfalls im IAPP ursprünglich definierten LLC Xid Pakete werden unabhängig von dieser Einstellung immer versendet wenn sich ein Client einbucht.

Aktiviere IAPP

Aktiviert IAPP Broadcasts und das empfangen von IAPP Nachrichten auf APs.

Aktiviere IAPP Client-Update

Aktiviert eine spezielle ads-tec Erweiterung des IAPP Protokoll. Dabei werden die Informationen des 802.11 Beacons zusätzlich im 1 Sekunden Intervall über das Ethernet als IAPP-Broadcast versendet. ads-tec Clients können diese Information empfangen und lernen so den Zustand und den aktuellen Kanal aller vorhandenen APs auch wenn diese evtl. noch nicht über Funk sichtbar sind. Diese Informationen sind vor allem beim Fastroaming nötig um die Kanalauflösung im 5 GHz Band automatisch abzuwickeln. Die Option ist daher nur sinnvoll wenn Fastroaming verwendet wird.

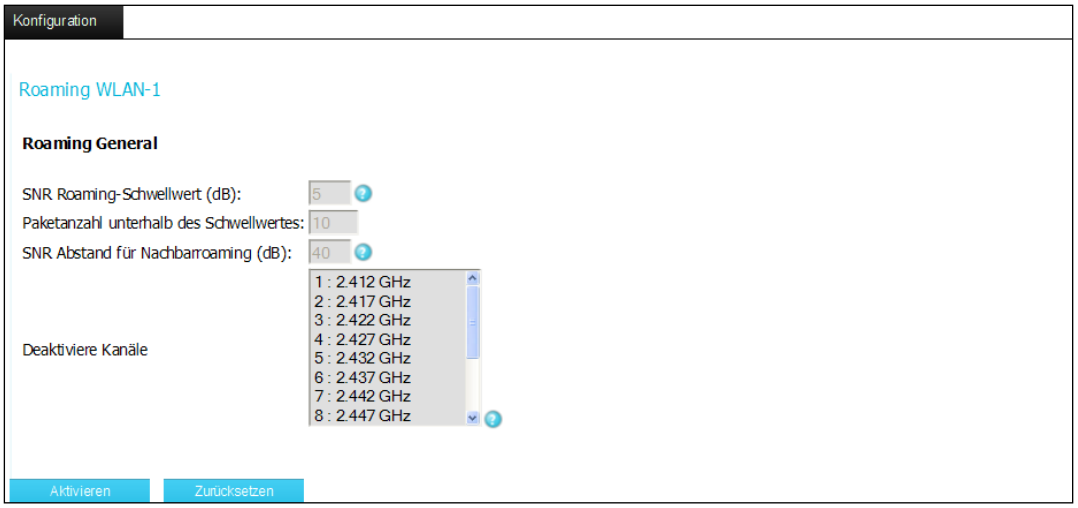
Hinweis:

Das IAPP (Inter-AccessPoint-Protokoll) wurde von der IEEE als 802.11f nicht vollständig definiert, später wurde der Draft zurückgezogen. IAPP ist daher kein Standardisiertes Protokoll.

ROAMING WLAN-1

Roaming Allgemein:

Roaming wird immer dann verwendet, wenn sich ein Client auf einer großen Fläche bewegt, die nicht nur von einem Access-Point abgedeckt wird. Im Vergleich zu Richtfunk oder Point to Point Verbindungen, die meist eine fixe Kanalwahl haben, müssen bei Roaming Setups die Clients in der Lage sein die verschiedenen Access-Points auf unterschiedlichen Kanälen zu finden. Die Einstellungen auf dieser Seite ermöglichen den Übergang von einem Netzwerk zum nächsten Netzwerk reibungslos und optimal einzustellen.



SNR Roaming-Schwellenwert:

Der Schwellenwert gibt an ab welchem db-Wert das Roaming ausgelöst wird. Sobald der hier angegebene Wert für eine gewisse Anzahl empfangener Pakete unterschritten wird, startet der Roaming- Vorgang.

Paketanzahl unterhalb des Schwellenwerts:

Gibt die Anzahl der Datenpakete für die Unterschreitung des obigen Wertes an.

SNR Abstand für Nachbarroaming:

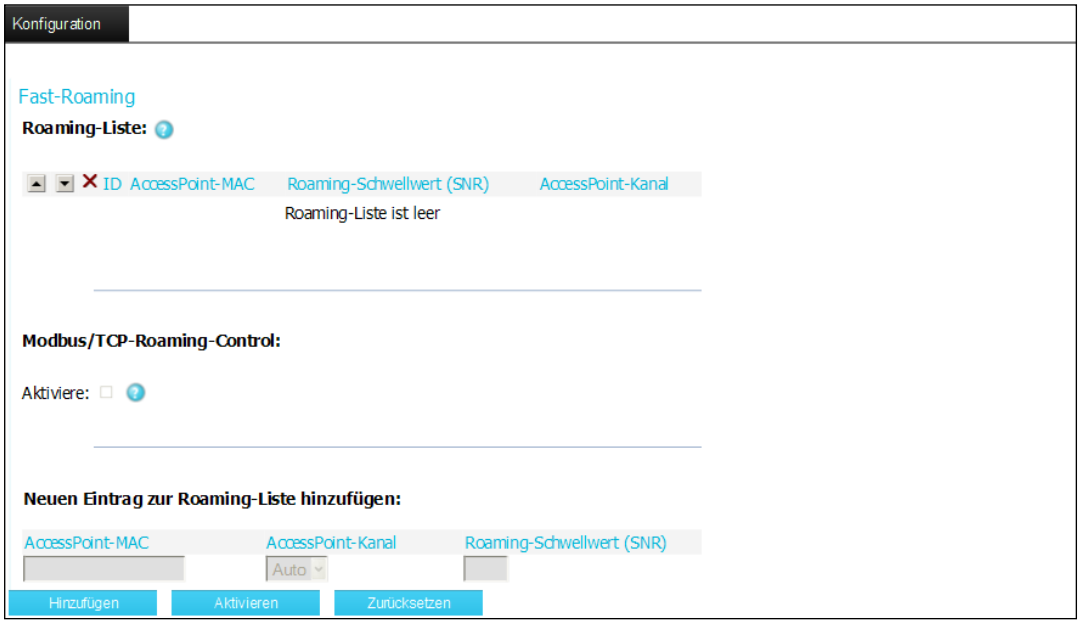
Der Client behandelt auch Pakete von anderen Access Points auf dem gleichen oder benachbarten Kanälen. Das Roaming zu einem solchen Access Point wird ausgelöst, sobald Pakete empfangen werden, deren SNR besser ist.

Hinweis:

Eine detaillierte Beschreibung zur optimalen Konfiguration der Roaming Funktion wird im Anwendungsbeispiel „Erweiterte Roaming Parameter“ dargestellt.

FAST-ROAMING

Die Funktion Fast Roaming ermöglicht ein gezieltes Einbuchen auf vorhandenen Access Points, ohne das ein Scan Vorgang gestartet wird.



Roaming- Liste:

Die Roaming- Liste enthält alle Access Points zu denen eine Verbindung hergestellt werden soll. Die Liste wird der Reihenfolge nach abgearbeitet. Der erste Eintrag wird auch als erster Verbindungsversuch verwendet.

Modbus/TCP-Roaming- Control:

Aktiviert die Modbus/TCP- API des Clients. Eine PLC kann dann die aktuelle Position in der Roaming-Liste abfragen oder Fast Roaming zu einem beliebeigen Eintrag in derRoaming- Liste auslösen.

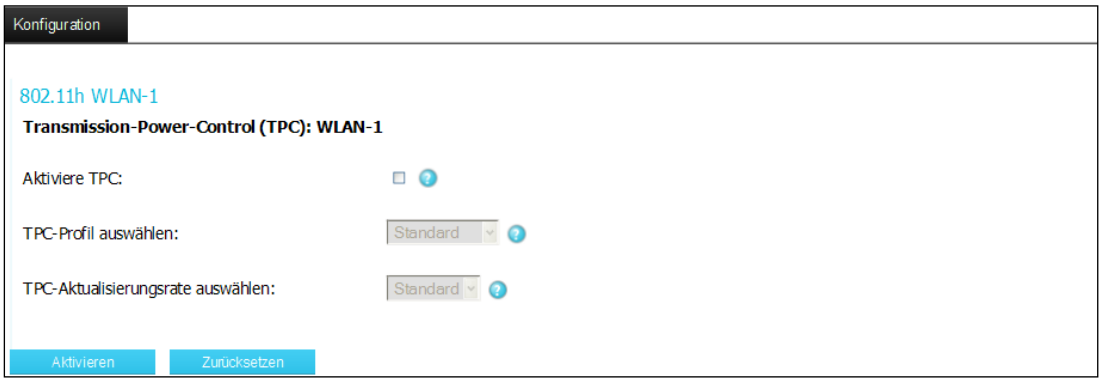
Neuen Eintrag zur Roaming- Liste hinzufügen:

Ermöglicht die Eintragung eines Access Points in die Roaming-Liste. Für die Eintragung wird die MAC-Adresse des Access Points benötigt. Desweiteren kann der Kanal (1-13) auf dem der Access Point erreichbar ist angegeben werden. Wenn der Kanal nicht bekannt sein sollte, kann die Auto Auswahl gewählt werden.

Die Fast Roaming Seite unterstützt Access-Points anderer Hersteller. Dies ist auch weiterhin möglich und insbesondere auf 5GHz mit DFS nötig um die dynamischen Kanäle zu verarbeiten. Auf 2.4 Ghz oder bei 5 Ghz mit deaktiviertem DFS kann man den Kanal des APs festvorgeben. Der Client wird dann nur diese APs in der gegebenen Reihenfolge und Roaming-Thresholds ablaufen. Kann ein AP nicht angesprungen werden fällt das Gerät in den Standard Scan Modus, und die anderen Roaming Parameter sind aktiv, wie z.B. die „Deaktivierten Kanäle“

802.11H WLAN-1

802.11h definiert eine Erweiterung des IEEE 802.11 WLAN-Standard um Zulassungskonforme Kommunikation auf dem 5 GHz Band in Europa zu ermöglichen. Der Standard beinhaltet zwei Komponenten: DFS: (Dynamic Frequency Selection) und TPC (Transmission Power Control). DFS wird schon auf der Standard WLAN Seite konfiguriert.



TPC:

Die Transmission Power Control hat zum Ziel die Sendeleistung eines Gerätes soweit möglich zu Reduzieren. TPC ist immer aktiv wenn ein 5 GHz Kanal verwendet wird, in diesem Fall kann TPC nicht abgeschaltet werden. Im 2.4 GHz Band ist TPC standardmäßig nicht aktiv, kann aber falls gewünscht aktiviert werden.

Power-Profile:

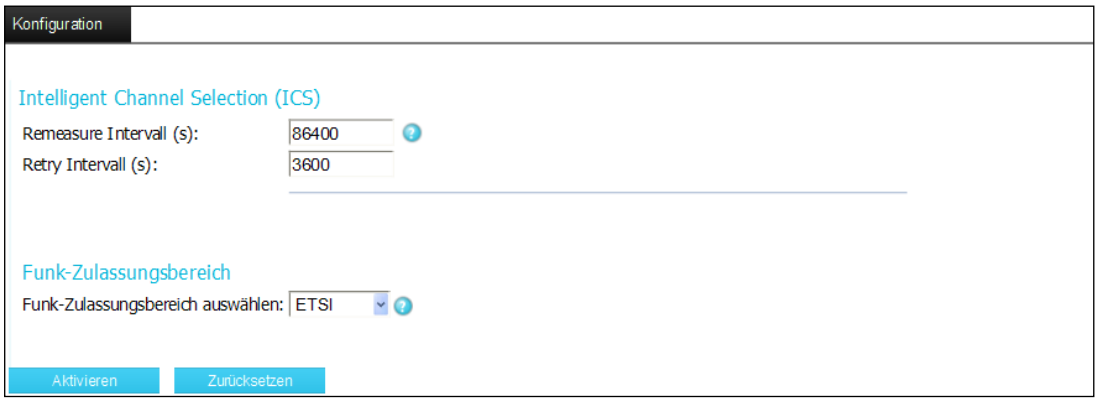
- Standard: Optimiert die Sendeleistung für die Datenrate von 48 MBit/s.
- Max. Power: Optimiert die Sendeleistung für die Datenrate von 54 MBit/s.
- Min. Power: Optimiert die Sendeleistung für die Datenrate von 11/12 MBit/s.

TPC- Aktualisierungsrate:

Sich schnell bewegende Clients sollten die hohe Aktualisierungsrate verwenden, da sonst die Verbindung abbrechen kann. Die niedrige Rate kann für statische Verbindungen verwendet werden.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

8.3.9 SONSTIGES



Remeasure Intervall:

Der Remeasure Intervall gibt an wann ein Gerät seine Umgebung neu ausmessen soll. Die Ausmessung wird nur durchgeführt wenn kein Client eingebucht ist. Falls ein Client eingebucht ist wird nach Retry Intervall Sekunden ein erneuter Versuch unternommen. Während der Ausmessung steht der AP nicht für WLAN Clients zur Verfügung.

Retry Intervall:

Falls ein Client eingebucht ist, wird der Remeassure Vorgang nach diesem Intervall erneut versucht, sind dann keine clienta mehr am Access Point eingebucht, kann dieser den Remeassure Vorgang starten.

Hinweis:

Die Remeassure Funktion kann mit dem Wert 0 in beiden Feldern deaktiviert werden.

Funk Zulassungsbereich:

Hier können die jeweils gültigen Ländereinstellungen zur Sendeleistung vorgenommen werden.

Achtung:

Der Betreiber des Gerätes ist verplfichtet, die korrekte Ländereinstellung zu wählen!

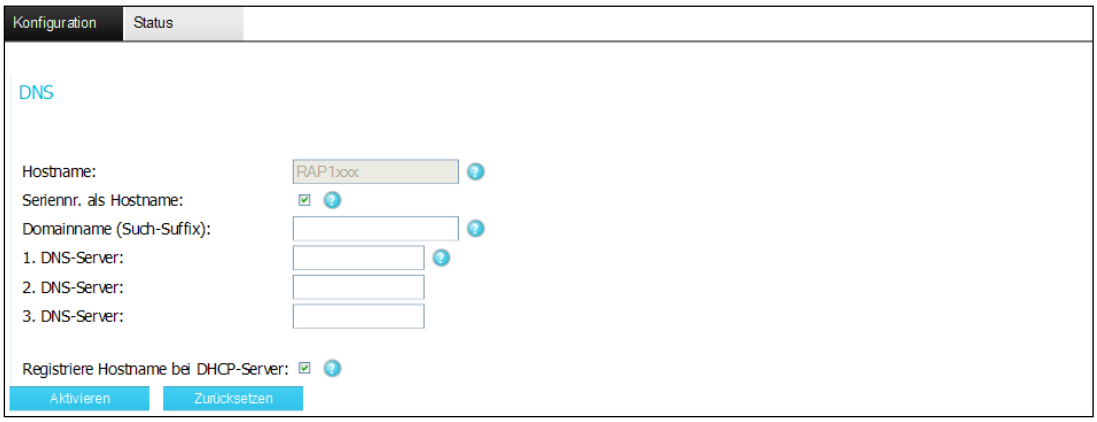
8.3.10 NETZWERK

DNS

Über die neue DNS Seite lassen sich die Nameserver und der Hostname des Gerätes konfigurieren. Die Nameserver werden nun verwendet wenn in einem Feld für IP-Adressen eines Servers (z.B. NTP Server) eine Hostname anstatt einer IP-Adresse verwendet wird). Der Hostname wird im Eventlog als Prefix verwendet.

Seriennr. als Hostname::

Diese Option ist standardmäßig aktiviert und zeigt den Systemname und die Seriennummer des Geräts an.



Hostname:

Der DNS Hostname des Gerätes selbst, wird z.B. bei Eventlog-Nachrichten verwendet.

Seriennr. als Hostname::

Diese Option ist standardmäßig aktiviert und sorgt für die Verwendung der Geräte-Seriennummer als Systemname.

Domainname (Such-Suffix):

Der Such-Suffix wird an alle DNS-Anfragen angehängt.

DNS-Server:

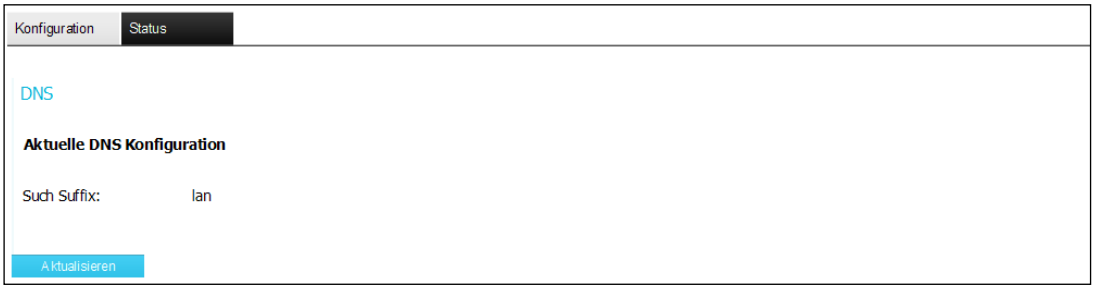
Es muss mindestens 1 DNS-Server konfiguriert werden um Hostnamen in IP-Adressen aufzulösen. Das Gerät verwendet dies um alle Hostnamen aufzuösen, die bei verschiedenen Parametern angegeben werden können.

Registriere Hostname bei DHCP-Server:

Falls aktiviert, wird bei jedem DHCP-Request des Gerätes der angegebene Hostname mit an den DHCP-Server übertragen.

Status:

Status:

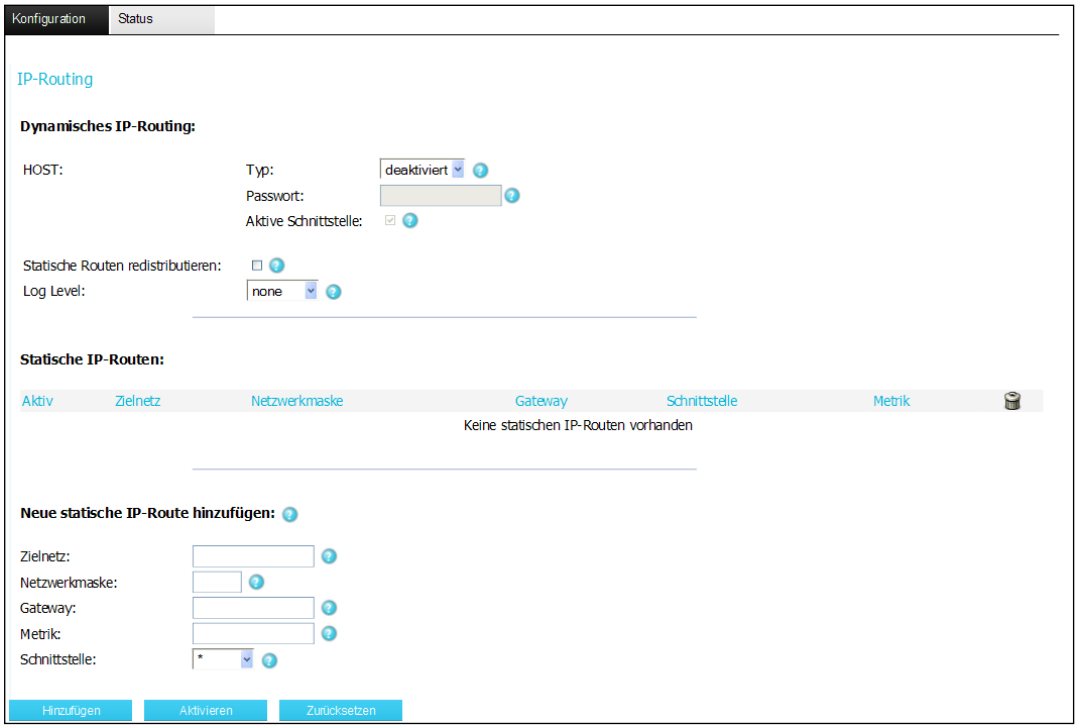


Hinweis:

Falls der DHCP-Server dynamische DNS-Updates nach RFC2136 unterstützt wird dies zu einem gültigem DNS Eintrag für den angegebenen Hostnamen auf dem DNS-Server führen.

Hinweis:
Wird eine Schnittstelle mit DHCP konfiguiert werden die hier manuell vorgenommenen Einstellungen dynamisch überschrieben.

IP-ROUTING



Dynamisches IP-Routing:

Hier kann ein spezielles Protokoll für das IP-Routing verwendet werden. Zur Auswahl stehen RIP:

häufig verwendetes Protokoll, dass die Erstellung der Routingtabelle für Router ermöglicht

OSPF:

Open Shortest Path First ist der Nachfolger des RIP-Protokolls.

Both: verwendet beide Protokolltypen

IP-Routing wird verwendet um IP-Pakete die zu einem Netzwerk gehören, an einen Gateway-Rechner weiterzuleiten. Ein Netzwerk besteht aus einer IP-Adresse und der zugehörigen Subnetzmaske. Die Werte sind unter Zielnetz und Netzwerkmaske einzutragen. Wenn die beiden zu verbindenden Netzwerke auf unterschiedlichen Protokollen basieren, muss das Gateway zusätzlich eingetragen werden.

PORT WEITERLEITUNG

Über den Menüpunkt **Port-Weiterleitung** ist es möglich, Verbindungen über frei wählbare Ports zu Computern/Adressen innerhalb eines Netzes weiterzuleiten oder zu initiieren.

Mit Port-Weiterleitung können Regeln definiert werden, die die eingehenden Ethernetpakete weiterleiten. Somit ist es möglich das „verschleierte“ Dienste (Ports) hinter dem Gerät direkt aus dem WLAN Netzwerk heraus anzusprechen, ohne dessen IP Adresse zu kennen. Port-Weiterleitung ist nur in den Router Betriebsmodi verwendbar. Die größte Bedeutung bekommt es in Zusammenspiel mit NAT und Extendend Background Scanning und IP Router.

Hinweis:

Für weitere Informationen, siehe entsprechendes Anwendungsbeispiel.

BRIDGE MODUS

Wenn das Gerät im Transparent Bridge Modus betrieben wird, erlaubt der Bridge Modus genauere Einstellmöglichkeiten.

Fully Transparent Bridge Modus:

Dieser Modus ist der Standard Transparent Bridge Modus, welcher auch im Paketfilteren auswählbar ist.

Multi Client Bridge:

Dieser Betriebsmodus ermöglicht das Betreiben eines WLAN-Clients an einem nicht ads-tec Access Point. Es werden alle Geräte welche am Ethernet des ads-tec Gerätes angeschlossen sind in Richtung WLAN mit der MAC-Adresse des WLAN Modules des ads-tec Gerätes automatisch maskiert. Das erste Gerät wird mit einem Layer 2 transparenten Zugriff maskiert, alle weiteren Geräte werden mit einem Layer 3 transparent maskiert, d.h. nur Protokoll-Daten können übertragen werden.

Single Client Bridge:

Hier kann genau ein Ethernet-Gerät hinter dem Client angeschlossen werden, welches mit Layer 2 transparent maskiert wird. Die MAC-Adresse des Geräts ist manuell einzutragen.

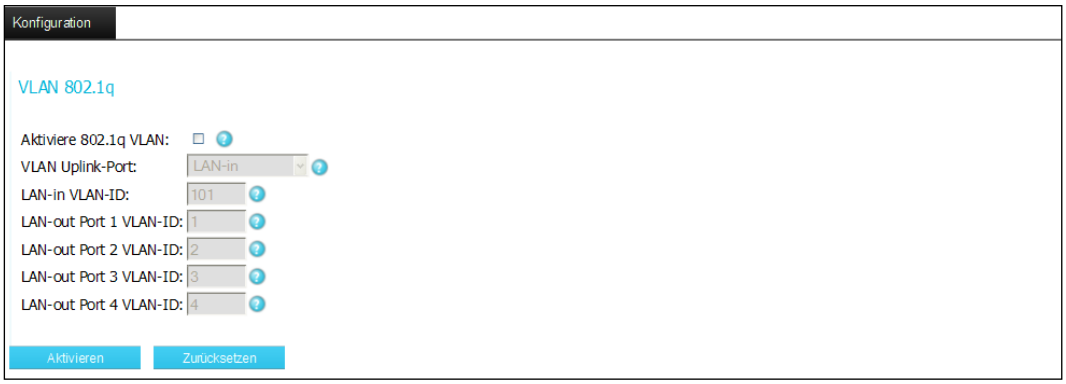
Hinweis:

Wenn im Single Bridge Modus oder im Multi Client Modus das ads-tec Gerät selbst als DHCP Client konfiguriert ist, können alle weiteren angeschlossenen Geräte ebenfalls DHCP verwenden. Das ads-tec Gerät startet automatisch einen DHCP-Relay, um entsprechende Anfragen weiterzuleiten.

VLAN 802.1Q

VLAN Kennungen (VLAN Tags) können mit Hilfe der eingebauten Firewallmechanismen genutzt werden um virtuelle Subnetze aufzubauen und den Datenverkehr zu trennen. Jedes Subnetz benutzt dazu eine eindeutige Nummer (VLAN-ID) um die Ethernetpakete zu kennzeichnen. Ein Gerät, das zum VLAN mit der ID=1 gehört, kann mit jedem anderen Gerät im gleichen VLAN kommunizieren, nicht jedoch mit einem Gerät in einem anderen VLAN mit ID=2, 3, ... Zusätzlich ist auch eine Priorisierung mit VLAN möglich. Es kann für jeden Frame eine Priorität (siehe Menüpunkt Priorisierung) angegeben werden. Dadurch ist es möglich, z. B. Steuerungsdaten bevorzugt weiterzuleiten, während HTTP-Daten ausgebremst werden.

Die Firewall verwendet einen Uplink-Port von dem aus die Pakete genau an einen anderen Zielport weitergeleitet werden. Ein Paket, das auf dem Zielport ankommt, wird mit der entsprechenden VLAN-ID auf dem Uplink-Port ausgegeben. Über die portweisen VLAN-IDs wird also jeweils ein VLAN Netzwerk zwischen Uplink und einem anderen Port aufgebaut.



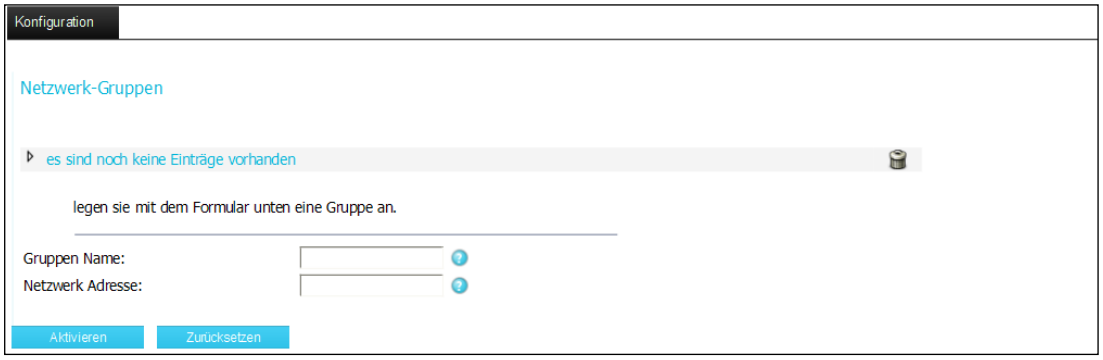
Die VLAN Funktionalität nach 802.1q wird mit der Option Aktiviere 802.1q VHOST Betrieb genommen.

Die Option Aktiviere Eingangsfilter verwirft alle Pakete mit VLAN Kennungen die nicht der Port VLAN-ID entsprechen.

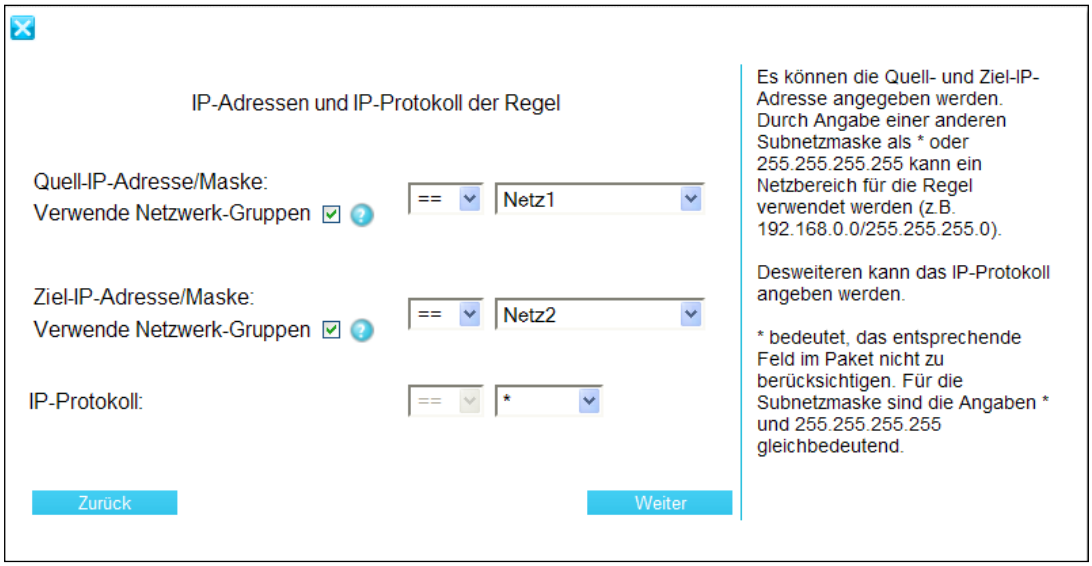
Die VLAN-Tags werden mit der Option Markierung ausgehender Pakete löschen auf einem Zielport entfernt bzw. gelöscht. Auf dem Zielport eingehende Pakete ohne Kennung werden mit der VLAN-ID des Ports versehen. Damit benötigt ein Gerät an einem Zielport keine spezielle VLAN-Konfiguration.

Die VLAN-ID kann für die Schnittstelle HOST sowie für die vier Ports des managed Switch HOST in den nachfolgenden Eingabefeldern eingegeben werden.

NETZWERK-GRUPPEN

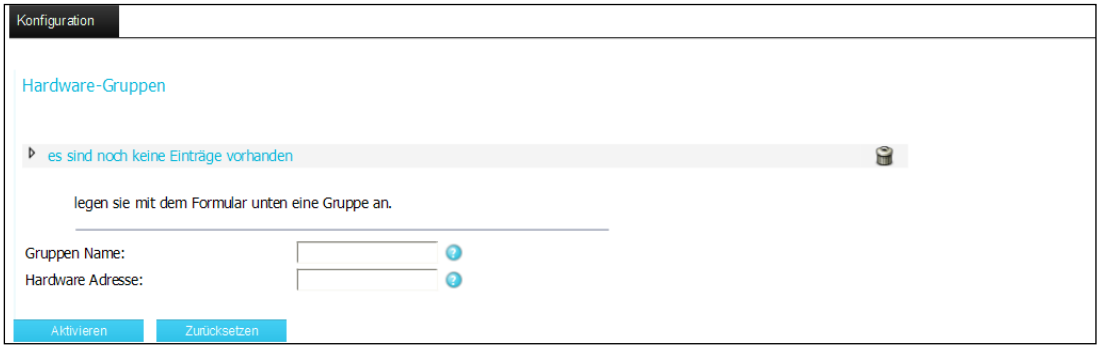


Die Netzwerkgruppen Funktion erlaubt eine Gruppierung von IP-Adressen und IP-Subnetzen um diese im Paketfilter für Filterregeln zu verwenden. Die Statuszeile gibt Informationen zu der Verwendung der Gruppe an. Wird eine Gruppe im Paketfilter einmal verwendet so wie die Statuszeile „Verwendung in 1 Regel“ ausgeben.

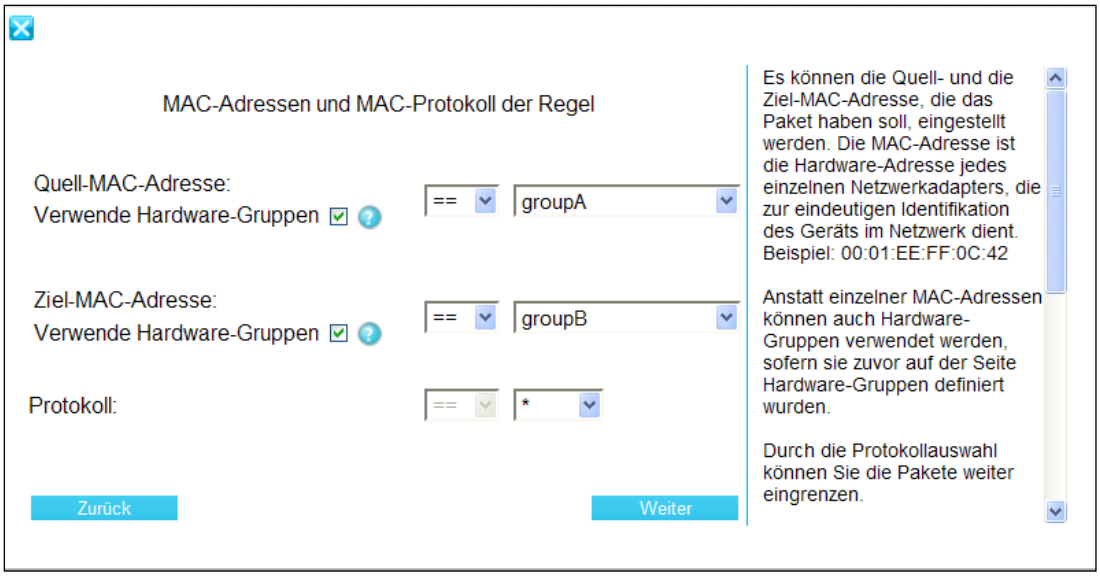

IP-Adressen und IP-Protokoll der Regel
Quell-IP-Adresse/Maske:
Verwende Netzwerk-Gruppen
==
Netz1
Ziel-IP-Adresse/Maske:
Verwende Netzwerk-Gruppen
==
Netz2
IP-Protokoll:
==
*
Zurück
Weiter
Es können die Quell- und Ziel-IP-Adresse angegeben werden. Durch Angabe einer anderen Subnetzmaske als * oder 255.255.255.255 kann ein Netzbereich für die Regel verwendet werden (z.B. 192.168.0.0/255.255.255.0).
Desweiteren kann das IP-Protokoll angeben werden.
* bedeutet, das entsprechende Feld im Paket nicht zu berücksichtigen. Für die Subnetzmaske sind die Angaben * und 255.255.255.255 gleichbedeutend.

Hinweis:
Die Verwendung von **!=** im Layer2 Filter Assistenten für Netzwerkgruppen wird nicht unterstützt.

HARDWARE-GRUPPEN



Die Hardwaregruppen Funktion erlaubt eine Gruppierung von MAC-Adressen um diese im Paketfilter für Filterregeln zu verwenden. Die Statuszeile gibt Informationen zu der Verwendung der Gruppe an. Wird eine Gruppe im Paketfilter ein mal verwendet, so wird die Statuszeile „Verwendung in 1 Regel“ ausgeben.


MAC-Adressen und MAC-Protokoll der Regel
Quell-MAC-Adresse:
Verwende Hardware-Gruppen
==
groupA
Ziel-MAC-Adresse:
Verwende Hardware-Gruppen
==
groupB
Protokoll:
==
*
Zurück
Weiter
Es können die Quell- und die Ziel-MAC-Adresse, die das Paket haben soll, eingestellt werden. Die MAC-Adresse ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Beispiel: 00:01:EE:FF:0C:42
Anstatt einzelner MAC-Adressen können auch Hardware-Gruppen verwendet werden, sofern sie zuvor auf der Seite Hardware-Gruppen definiert wurden.
Durch die Protokollauswahl können Sie die Pakete weiter eingrenzen.

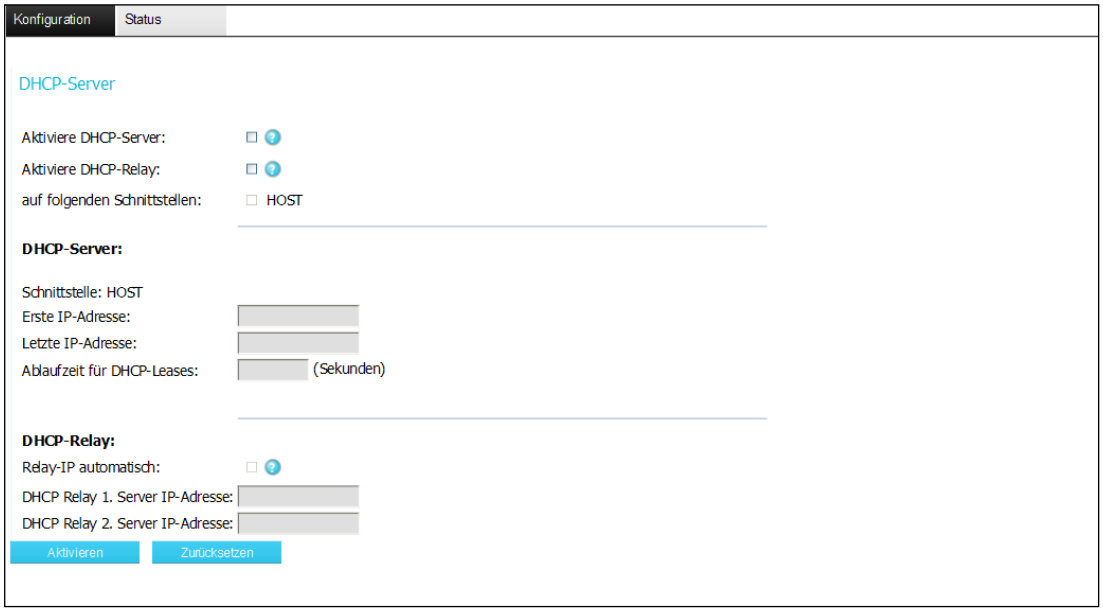
Hinweis:

Hardwaregruppen lassen sich nur in Layer2 Regelsätzen verwenden, da nur dort eine Filterung auf MAC-Adressen möglich ist.

8.3.11 DIENSTE

DHCP-SERVER

Der eingebaute DHCP-Server kann für die Verteilung von IP-Adressen benutzt werden. Als Standardeinstellung ist er jedoch abgeschaltet und kann durch die Option **Aktiviere DHCP-Server** in Betrieb gesetzt werden.

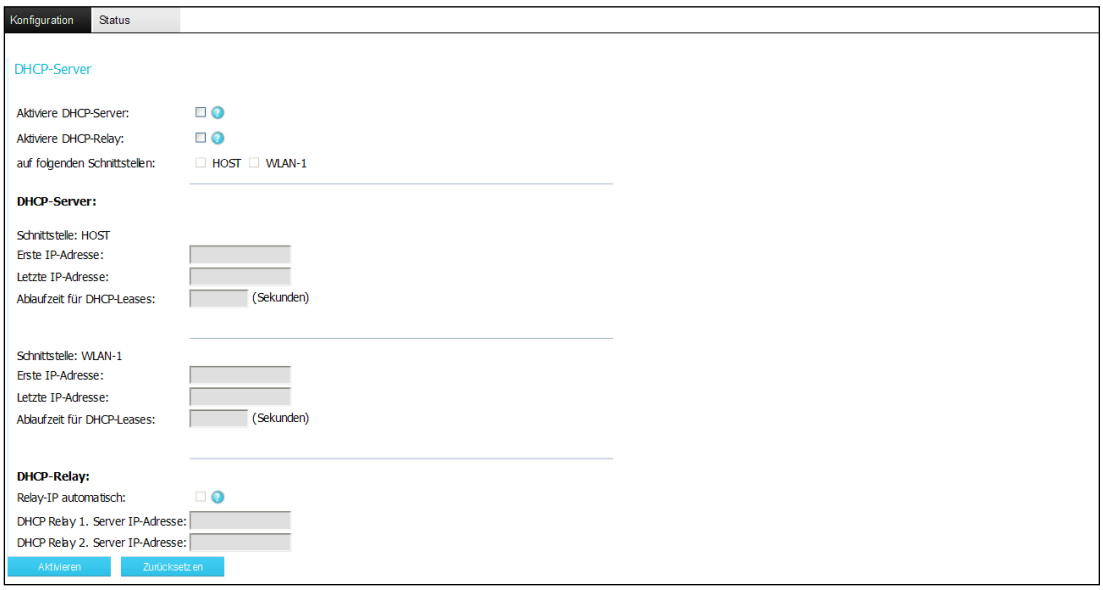


Hinweis:

Der IP-Adressbereich muss im gleichen Bereich liegen wie die IP-Adresse der verwendeten Schnittstelle selbst!

Die Schnittstellen auf denen der DHCP-Server Anfragen von Clients beantworten soll, können in den Optionen **auf folgenden Schnittstellen** detaillierter spezifiziert werden. Der Poolbereich lässt sich pro Schnittstelle separat einstellen.

Zusätzlich zur Verteilung von IP-Adressen kann der DHCP-Server auch im Serverbetrieb ein Domain Such-Suffix sowie drei DNS-Serveradressen übermitteln. Diese Informationen werden an DHCP-Clients weitergereicht. Das Gerät benutzt einen eigenen DNS-Dienst um alle Anfragen zwischenzuspeichern. Arbeitet der Access Point selber nicht mit einer statischen IP-Adresse sondern als DHCP-Client werden diese Daten durch den dann verwendeten DHCP-Server überschrieben.



(Ansicht IP-Router)

DHCP-RELAY:

Im IP-Router Modus besteht die Möglichkeit alternativ zu einem DHCP-Server einen DHCP-Relay Server zu Aktivieren. Der DHCP-Relay Server dient der Weiterleitung von DHCP-Anfragen über ein Ethernet-Segment hinweg. Im DHCP-Relay Betrieb müssen alle Schnittstellen auf denen DHCP-Anfragen empfangen werden sowie die Schnittstelle auf der der eigentliche DHCP läuft ausgewählt werden.

Relay-IP automatisch:

Bei aktivierter Funktion arbeitet der Access Point selbst als DHCP-Server und antwortet auf Anfragen von der ausgewählten Schnittstelle.

Relay IP-Adresse:

Hier ist dier IP-Adresse des DHCP-Servers einzutragen.

SNMP

Durch das Simple Network Management Protocol (SNMP) ist es möglich, Netzwerkgeräte wie z.B. Router, Switches oder Server über einen zentralen Punkt zu verwalten und zu überwachen. Das Protokoll regelt nicht nur die Kommunikation zwischen dem überwachten Gerät und der Überwachungsstation, sondern ermöglicht auch eine Fehlererkennung und Benachrichtigung.

SNMP AKTIVIEREN:

Aktiviert oder Deaktiviert das SNMP Protokoll.

SNMPv1/v2:

Bei aktivierter Funktion wird die erste und zweite Protokollversion verwendet, welche allerdings unverschlüsselt und somit nicht sicher genug ist.

SNMPv3:

Bei aktivierter Funktion wird die dritte Version des SNMP Protokolls verwendet, welche einen zusätzlichen Schutz durch Vergabe eines Benutzernamens und eines Passworts bietet.

SNMP NUR-LESE ZUGRIFF / SNMP LESE-/SCHREIB-ZUGRIFF:

Hinweis:
Wählen Sie entsprechend ihren Anforderungen, ob Sie nur Lese,- oder Lese/Schreibrechte konfigurieren möchten und füllen Sie die entsprechende Maske mit ihren Daten aus.

SNMP Community Name:

Der hier einzutragende Name ist vergleichbar mit einem Passwort. Gängige Default Einstellungen sind private oder public.

SNMP Community IP:

Der Zugriff mit angegebenem Community Namen wird auf folgende IP-Adresse beschränkt.

Hinweis:
Um alle Quell-IPs zuzulassen, wählen Sie die IP: **0.0.0.0**

SNMP Community Netz Maske:

Hier ist die entsprechende Netz-Maske zur IP-Adresse einzutragen.

SNMPv3 Benutzername und Verschlüsselung:

Hinweis:
Diese Funktion steht nur zur Verfügung wenn SNMPv3 ausgewählt ist. Wählen Sie entsprechend ihren Anforderungen, ob Sie nur Lese,- oder Lese/Schreibrechte konfigurieren möchten und füllen Sie die entsprechende Maske mit ihren Daten aus.

Benutzername:

Vergeben Sie einen Benutzernamen für die Authentifizierung mit dem SNMPv3 Protokoll

Passwort:

Vergeben Sie zu ihrem Benutzernamen ein Passwort.

Hinweis:
Das verwendete Authentifizierungsprotokoll bei dieser Anmeldung ist MD5.

Pre-shared key:

Der Pre-Shared Key ist ein Schlüssel, bestehend aus einer Kombination aus Zahlen oder Buchstaben, welcher zusätzlich zu Benutzername und Passwort verwendet werden kann. Über den Button „**PSK-Erstellen**“ kann ein zufällig generierter Zahlencode erstellt werden, der für den Pre-Shared Key verwendet werden kann.

SNMP TRAP ERZEUGUNG AKTIVIEREN:

Ermöglicht das Aktivieren/Deaktivieren der SNMP Trap Funktion. Bei eingeschalteter Funktion können Ereignisse wie z.B. Link Up / Link Down empfangen und nachvollzogen werden. Durch das Mitsenden der IP-Adresse kann nachvollzogen werden von welchem Gerät die Meldung kommt.

SNMP Trap Community Name:

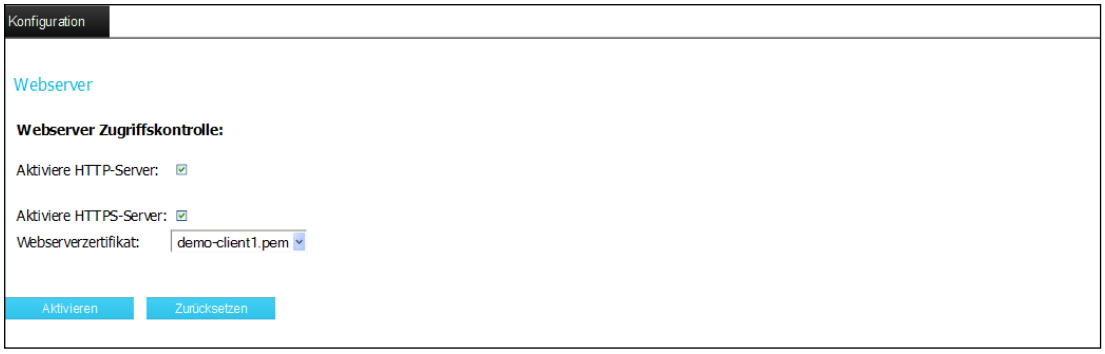
Hier ist der Community Name für Traps einzugeben.

SNMP Trap IP Empfänger:

Tragen Sie hier die IP-Adresse des Trap Empfängers ein.

WEBSERVER

Über das Menü Webserver Zugriffskontrolle kann der Zugriff auf die Access Point Weboberfläche mit den Protokollen http bzw. https eingestellt werden.



Der im Access Point für die Konfiguration integrierte Webserver wird nur bei den aktivierten Protokolloptionen erreichbar sein.

Hinweis:

Für optimierte Sicherheit sollte jeder Access Point ein eigenständiges individuelles Zertifikat zugeordnet werden.

CLIENT- MONITORING

Die eingebaute Funktionalität des Client-Monitoring dient der Überwachung von Teilnehmern auf ihre Verfügbarkeit im Netzwerk. Die zu überwachenden Clients werden zur Client Monitoring-Tabelle hinzugefügt und werden zyklisch per ICMP-Nachrichten auf Erreichbarkeit überprüft.

Ein zu überwachender Client kann bei Verlust der Erreichbarkeit eine Aktion auslösen. Die Aktion kann z.B. das Versenden einer E-Mail an den jeweiligen Zuständigen sein.

Aktion:

up/down WLAN-1/2

Kann der Ethernet Teilnehmer nicht mehr via ICMP erreicht werden wird durch diese Einstellung der WLAN Adapter heruntergefahren. Wird der ICMP auf dem Gateway des APs ausgeführt kann der AP nun erkennen das er keinen Uplink mehr hat. Das HOST Interface fährt nun runter und wirft damit alle Clients raus. Ansonsten kann es passieren das ein Client sich einbucht obwohl der AP keine Konvektivität hat und der Client besser einen anderen AP suchen sollte.

Hinweis:

Soll die aktuelle Zeit der ICMP-Antworten überprüft werden, so kann im Feld Status ein Tooltip auf einer symbolischen LED abgerufen werden.

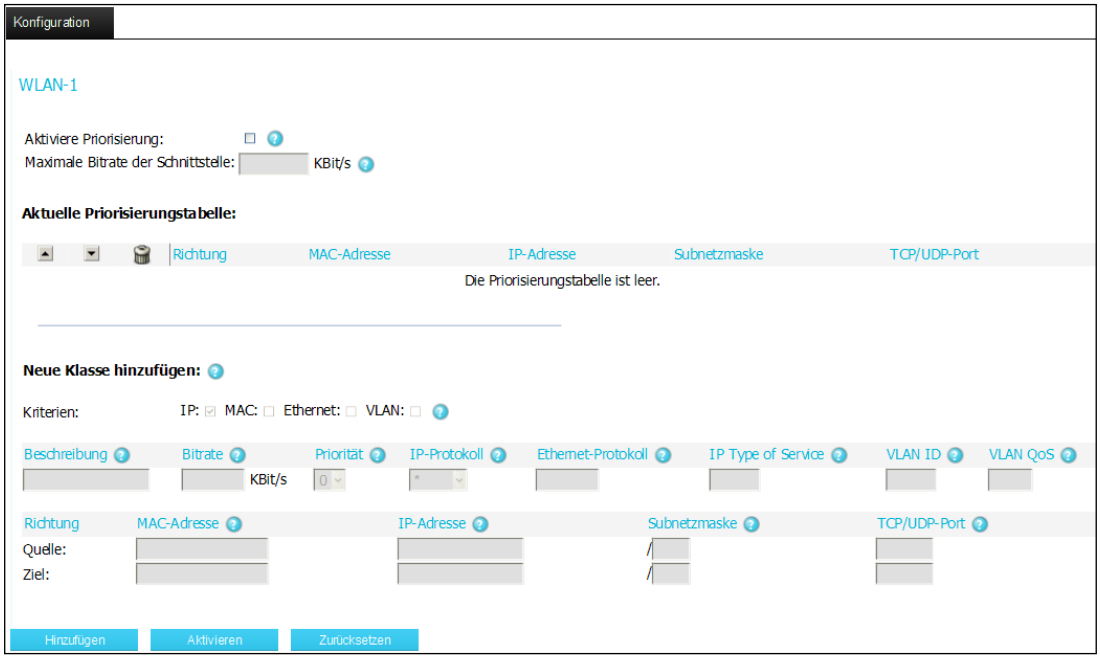
Hinweis:

Wird im Optionsfeld E-Mail-Server und E-Mail-Adresse eine gültige Adresse hinterlegt, so wird eine Statusänderung per E-Mail signalisiert.

8.3.12 PRIORISIERUNG

WLAN 1

Die im Access Point integrierte Priorisierungsfunktion dient zur differenzierten Behandlung von Datenströmen zwischen verschiedenen Schnittstellen. Hiermit ist es möglich Datenpakete bevorzugt zu behandeln oder bestimmte Protokolle in ihrer Bandbreite zu limitieren.



Aktiviert wird die Priorisierungsfunktion durch Eingabe einer maximalen Bitrate sowie mindestens einer Priorisierungsklasse. So ist z.b. eine maximale Bitrate von 51200KBit/s einzugeben, wenn die angeschlossene Ethernet Infrastruktur einen maximalen Durchsatz von 50MBit/s bietet. Die Kritieren für die Priorisierungsklassen sind nicht in allen Varianten kombinierbar. So ist eine Auswahl von IP mit VLAN durch das Funktionsprinzip ausgeschlossen. Die Priorisierung auf WLAN Schnittstellen verwendet WMM Funktionen. WMM Priorisierung ist Standardmäßig aktiviert und kann nicht abgeschaltet werden. Die IP ToS Felder und VLAN QoS Tags werden nach der WMM Spezifikation auf 4 verschiedene Queues verteilt. Wenn man unabhängig von den IP ToS oder VLAN QoS Tags Pakete klassifizieren möchte, so kann man nun dazu die Priorisierungseite verwenden. Das Feld Priority wird in die 4 WMM Klassen abgebildet:

0,1 -> WMM Voice

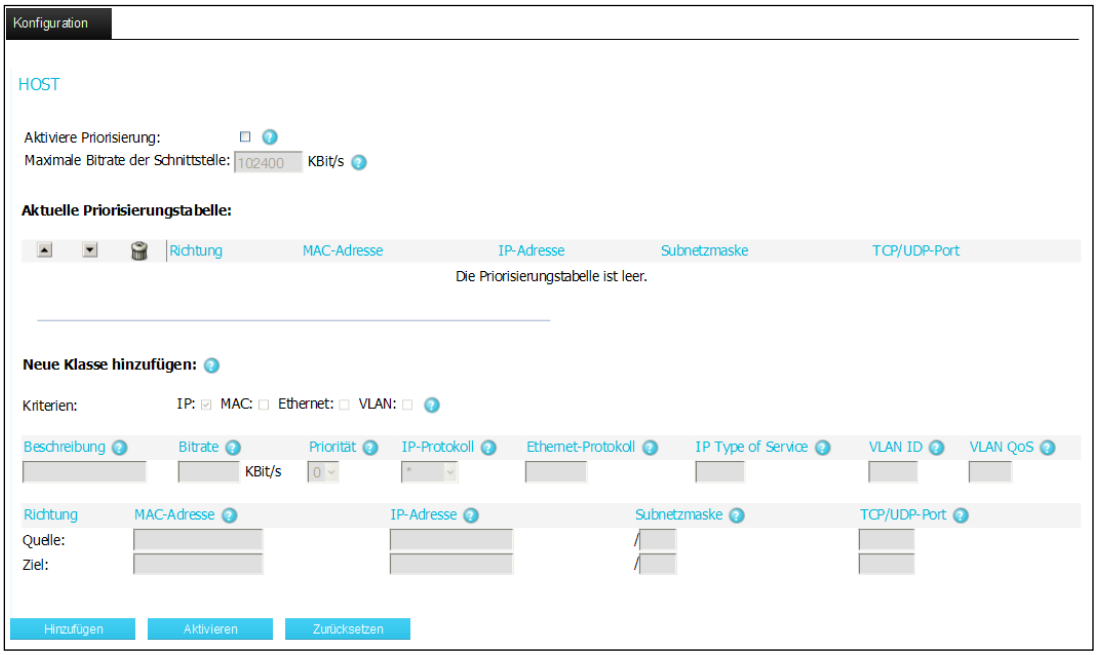
2,3 -> WMM Video

4,5 -> WMM Best Effort

6,7 -> WMM Background

Die Lend Bitrate Funktion und die Funktion Dynamic Bitrate wurden entfernt um die Bedienung einfacher zu machen. (Lend Bitrate ist nun per Default abgeschalten)

HOST



Hinweis:

Soll ein spezifischer Datenstrom priorisiert werden, so müssen mindestens zwei Klassen angelegt werden. Die erste anzulegende Klasse erhält den kleinsten Prioritätswert im Optionsfeld **Priorität** und spezifiziert hiermit den bevorzugten Datenverkehr. Die zweite Klasse spezifiziert den restlichen Datenstrom und sollte eine von der maximalen Bitrate reduzierten Wert erhalten. Hiermit ist sichergestellt, dass der priorisierte Datenverkehr der ersten Klasse genügend Bandbreite erhält.

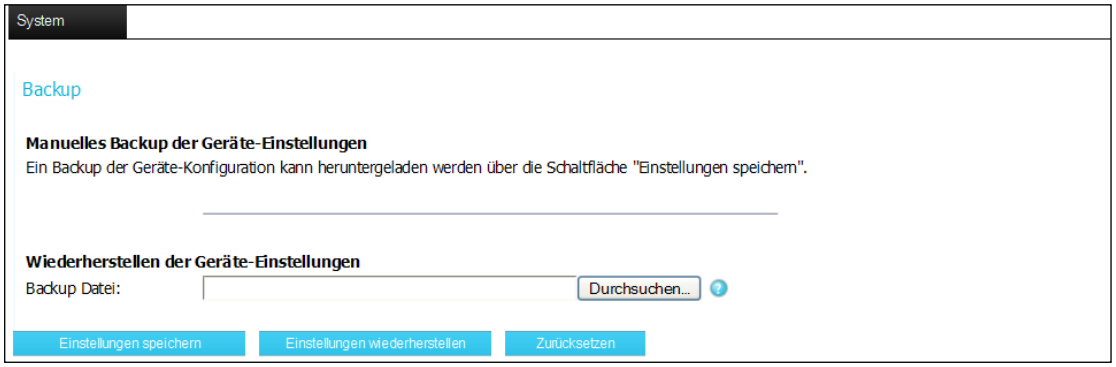
Hinweis:

Im Eingabefeld **Priorität** symbolisiert ein numerisch kleiner Wert die geringste Wartezeit der Ethernetpakete, während ein hoher Wert einer höheren Wartezeit entspricht!

8.4 HAUPTMENÜPUNKT SYSTEM

8.4.1 BACKUP EINSTELLUNGEN

Über Backup-Einstellungen können Sie eine Sicherung bzw. das Wiederherstellen der Geräte-Konfiguration vornehmen. Diese kann bei Verwendung von gleichen Firmwareständen auch auf mehrere Geräte aufgespielt werden.

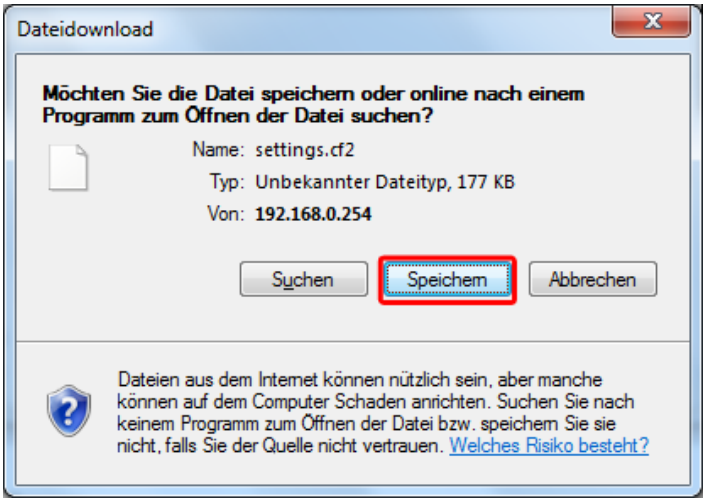


SICHERN DER GERÄTEKONFIGURATION

Um ihre Einstellungen in einer Datei zu sichern, klicken Sie auf: **Einstellungen speichern**.

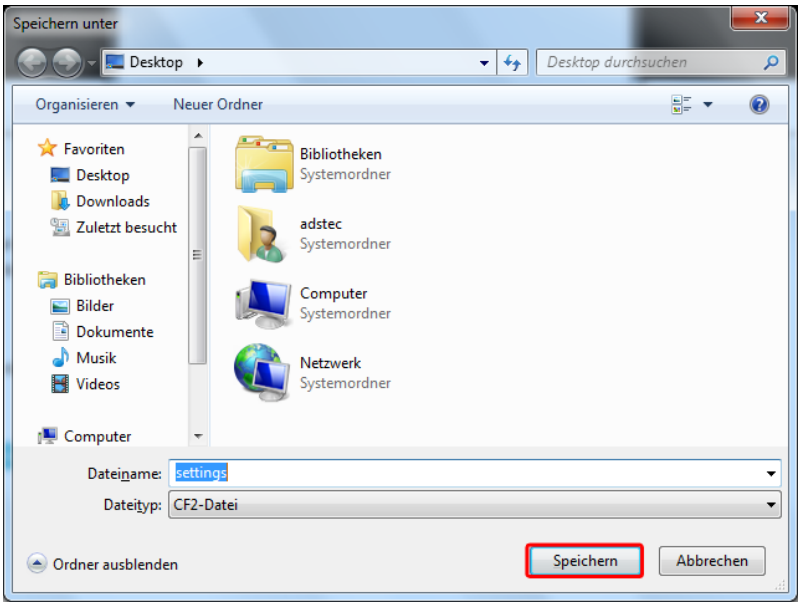
Hinweis:

Der Dateiname ist vordefiniert und kann nicht in der Weboberfläche vorgegeben werden. Eine Änderung des Dateinamens kann beim festlegen des Speicherortes vorgenommen werden. Die Dateiendung *.cf2 darf nicht abgeändert werden.


Dateidownload
Möchten Sie die Datei speichern oder online nach einem Programm zum Öffnen der Datei suchen?
Name: settings.cf2
Typ: Unbekannter Dateityp, 177 KB
Von: 192.168.0.254
Suchen
Speichern
Abbrechen
Dateien aus dem Internet können nützlich sein, aber manche können auf dem Computer Schaden anrichten. Suchen Sie nach keinem Programm zum Öffnen der Datei bzw. speichern Sie sie nicht, falls Sie der Quelle nicht vertrauen. Welches Risiko besteht?

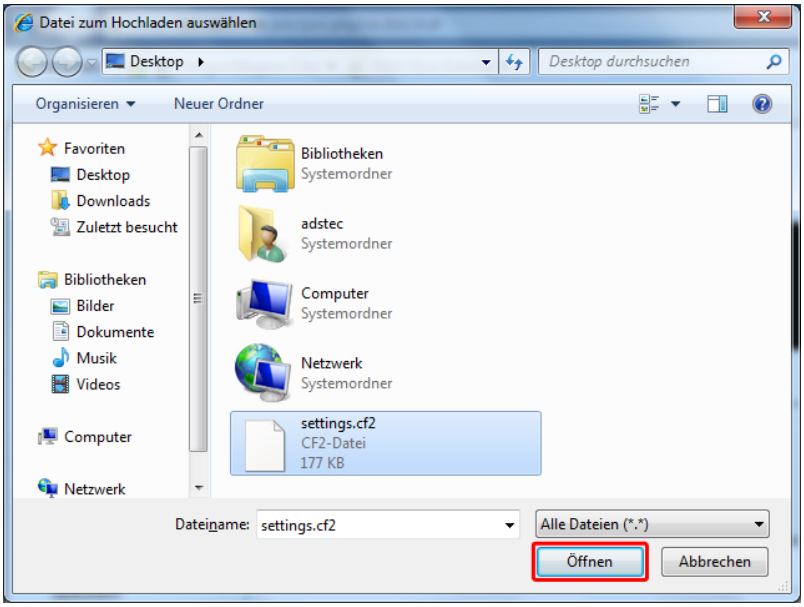
Wähen Sie Einstellungen speichern

Sie werden aufgefordert, die Datei **settings.cf2** zu speichern. Klicken Sie auf **Speichern** und wählen Sie anschließend einen Speicherort aus und klicken erneut auf **Speichern**.



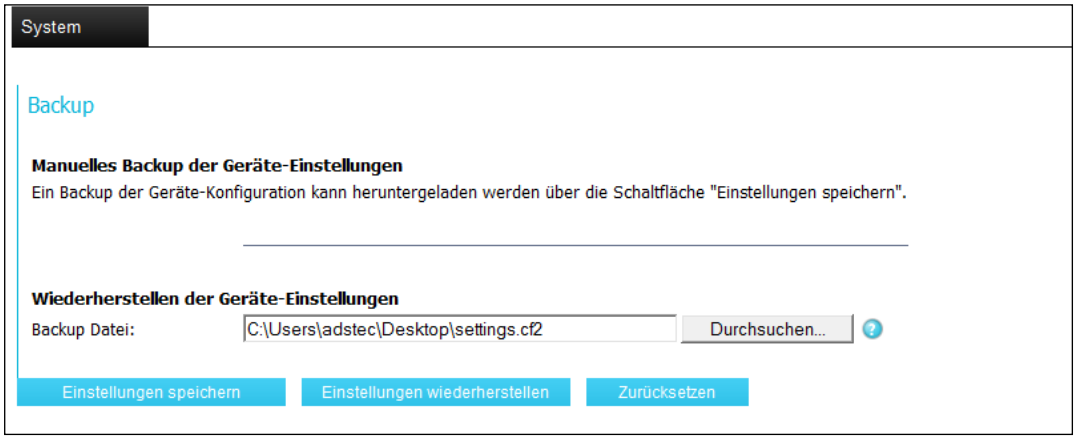
WIEDERHERSTELLEN DER GERÄTEKONFIGURATION

Um ihre gesicherten Einstellungen zu laden, klicken Sie auf **Durchsuchen** und wählen die Datei **settings.cf2** aus.



Bestätigen Sie mit **Öffnen**.

Klicken Sie anschließend auf den Button: **Einstellungen wiederherstellen**.



Nach dem Neustart des Geräts sind die Einstellungen geladen bzw. wiederhergestellt.

8.4.2 SOFTWAREUPDATE

Über Softwareupdate kann die Firmware des Gerätes aktualisiert werden. Dies kann auf drei verschiedenen Wegen erfolgen:

AKTUALISIERUNG VIA ONLINE UPDATE

Über die Schaltfläche **Check** kann überprüft werden, ob eine Aktualisierung vorliegt. Um diese Funktion nutzen zu können muss die ads-tec Website via http erreichbar sein.

AKTUALISIERUNG VON FIRMWARE SERVER

Es besteht die Möglichkeit, die Firmware über einen FTP-, TFTP, oder HTTP-Server zu aktualisieren.

AKTUALISIERUNG VIA BROWSER UPLOAD

Wenn die Datei lokal abgespeichert wurde besteht die Möglichkeit die Firmware-Datei direkt auszuwählen. Bestätigen Sie ihre Auswahl mit **Upload durch den Browser-Upload**.

VORGEHENSWEISE:

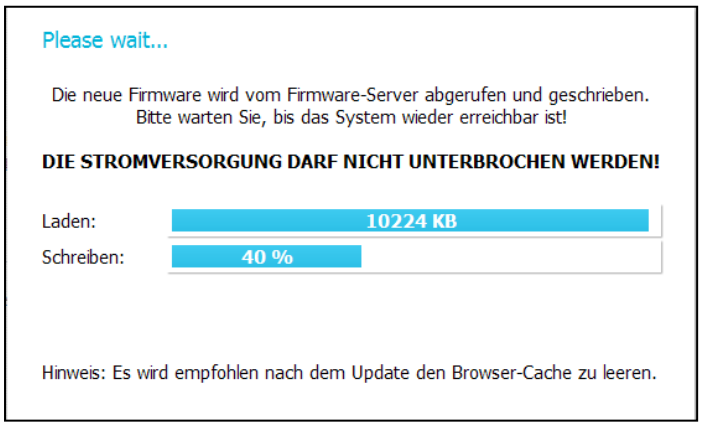
1) Speichern Sie die Firmwaredatei in einem lokalen Ordner ihrer Wahl auf dem PC ab.
2) Starten Sie den gewünschten Serverdienst oder verwenden sie ein Freewareprogramm wie tftpd32 um ein Firmware-Update durchzuführen. Beachten sie auch lokale Geräteeinstellungen auf ihrem PC damit die Kommunikation zum Gerät nicht blockiert wird.
3) Geben Sie nun unter **Browse** den Pfad des Ordners an, in dem sich die neue Firmware befindet und bestätigen Sie mit **OK.**

Hinweis:

Vergewissern Sie sich das die Dateiendung (.bin) der Firmware angegeben ist.
Beispiel: Ads-tec-RAPxxx-X.X.X-SVN-R10923M.B-7251**.bin**

4) Bevor Sie den Updatevorgang starten, wird empfohlen die Werkseinstellungen der neuen Firmware zu übernehmen.
5) Starten Sie den Updatevorgang über **Upload von Firmware-Server**

Während des Firmware-Updates erscheint dieses Dialogfenster.


Please wait...
Die neue Firmware wird vom Firmware-Server abgerufen und geschrieben.
Bitte warten Sie, bis das System wieder erreichbar ist!
DIE STROMVERSORGUNG DARF NICHT UNTERBROCHEN WERDEN!
Laden:
10224 KB
Schreiben:
40 %
Hinweis: Es wird empfohlen nach dem Update den Browser-Cache zu leeren.

Sobald die Link LED auf dem ausgewählten Port konstant grün leuchtet und die ACT-LED erloschen ist, kann der Button: **Versuche erneut zu verbinden** bestätigt werden.

Das Gerät versucht nun, auf die Weboberfläche zuzugreifen. Wenn das Update erfolgreich verlaufen ist, erscheint die Anzeige des Softwareupdates.

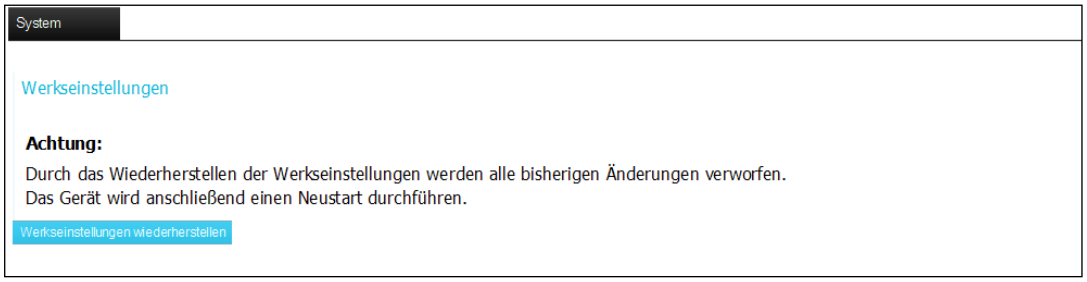
Achtung:

Die Stromversorgung darf auf keinen Fall während dieses Vorgangs unterbrochen werden!

8.4.3 WERKSEINSTELLUNGEN

Dieser Menüpunkt erlaubt das Wiederherstellen der Werkseinstellungen per Software.

Durch Klick auf den Button **Werkseinstellungen wiederherstellen** werden die Standard-Einstellungen des Gerätes geladen.



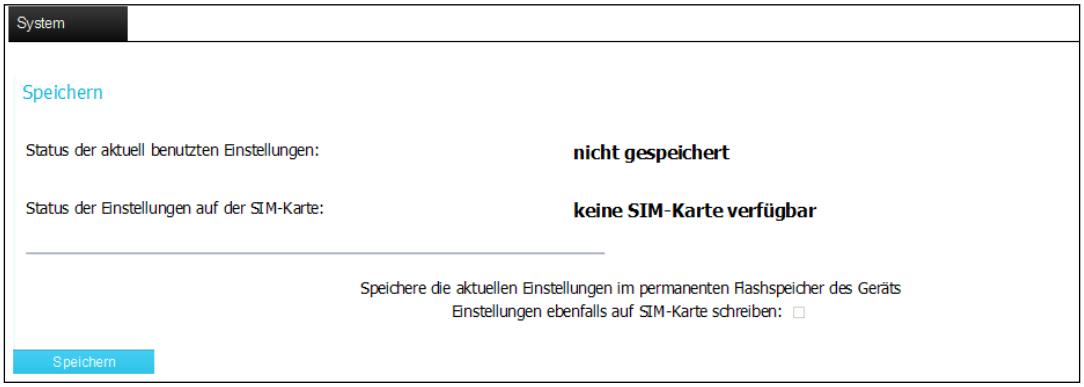
Über das dann erscheinende Webfenster können Sie auf **Versuche neu zu verbinden** klicken.Das Gerät versucht nun, auf die Weboberfläche zuzugreifen. Wenn das Update erfolgreich verlaufen ist, erscheint die Anzeige des Softwareupdates.

Achtung:
Es werden alle Einstellungen zurückgesetzt. Alle neu angelegten Filterregeln werden gelöscht. Sollten Sie nach dem Zurücksetzen auf die Werkseinstellungen nicht mehr auf die Weboberfläche gelangen, muss ggf. auch die IP-Adresse ihres PCs angepasst werden.

Folgende Standardeinstellungen werden eingestellt:

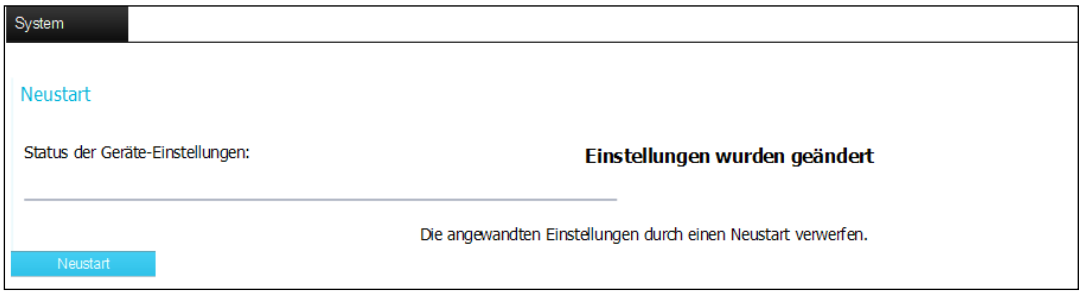
- Transparentbridge Betriebsmodus
- IP 192.168.0.254
- Benutzername: **admin**
  Passwort: **admin**

8.4.4 SPEICHERN



Über Speichern können alle getätigten Systemeinstellungen gespeichert werden. Zusätzlich können die Einstellungen auf der Sim-Karte abgelegt werden.

8.4.5 NEUSTART



Führt einen Neustart des System durch.

8.6 HAUPTMENÜPUNKT INFORMATIONEN

8.6.1 ALLGEMEIN

Der Menüpunkt **Allgemein** zeigt grundlegende Informationen zum Gerät.

HERSTELLER:

Das Feld zeigt alle relevanten Informationen zum Hersteller ads-tec GmbH.

GERÄTEINFORMATIONEN:

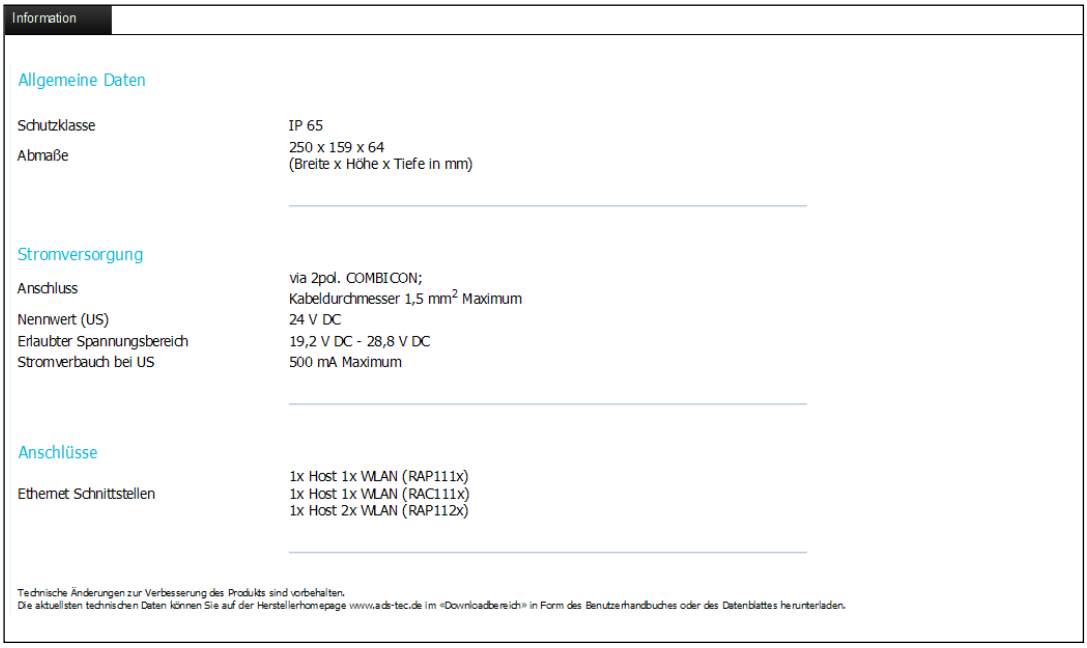
Die Geräteinformationen zeigen alle relevanten Daten zum Gerät wie z.B. Typ, Firmwareversion und Hardware-Version.

BENUTZERDEFINIERT:

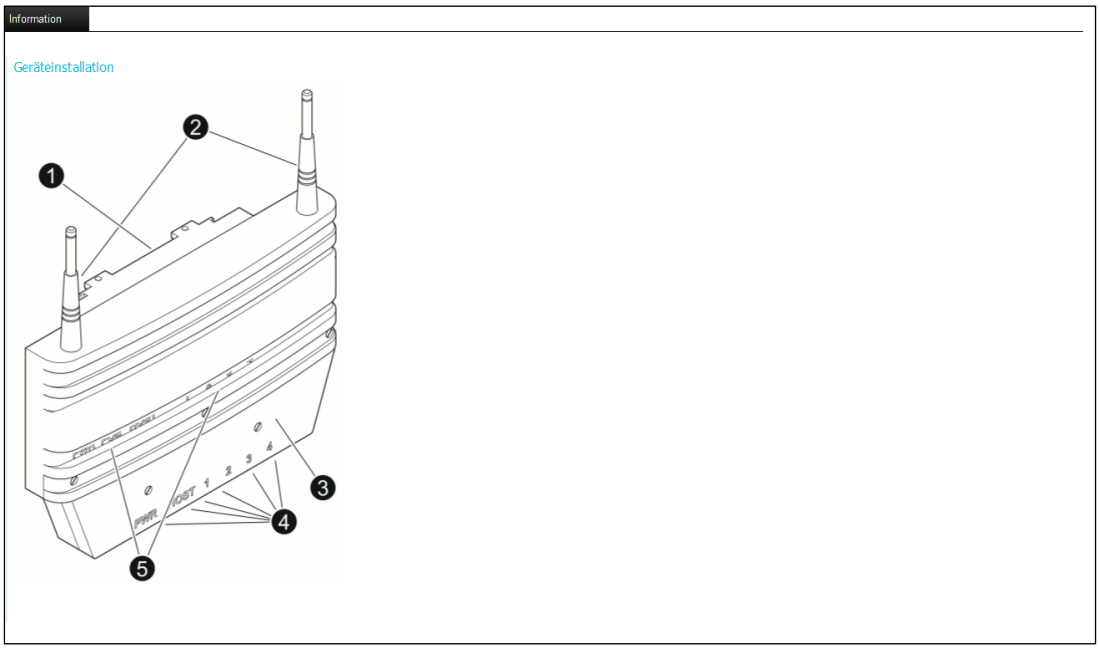
Die Rubrik Benutzerdefiniert zeigt kundenspezifische Daten des Geräts an.

8.6.2 TECHNISCHE DATEN

Der technische Daten Screen zeigt allgemeine Daten zur Inbetriebnahme, sowie die zulässige Spannungsversorgung des Geräts an.



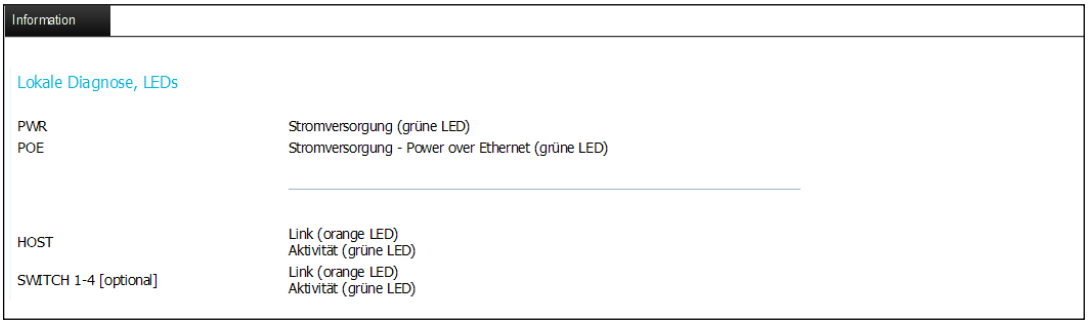
8.6.3 GERÄTEINSTALLATION



1) Montageplatte (Befestigung des Access Point an der Montagestelle)
2) Antenne
3) Service-Schacht
4) Schnittstellen
5) Status-Anzeigen

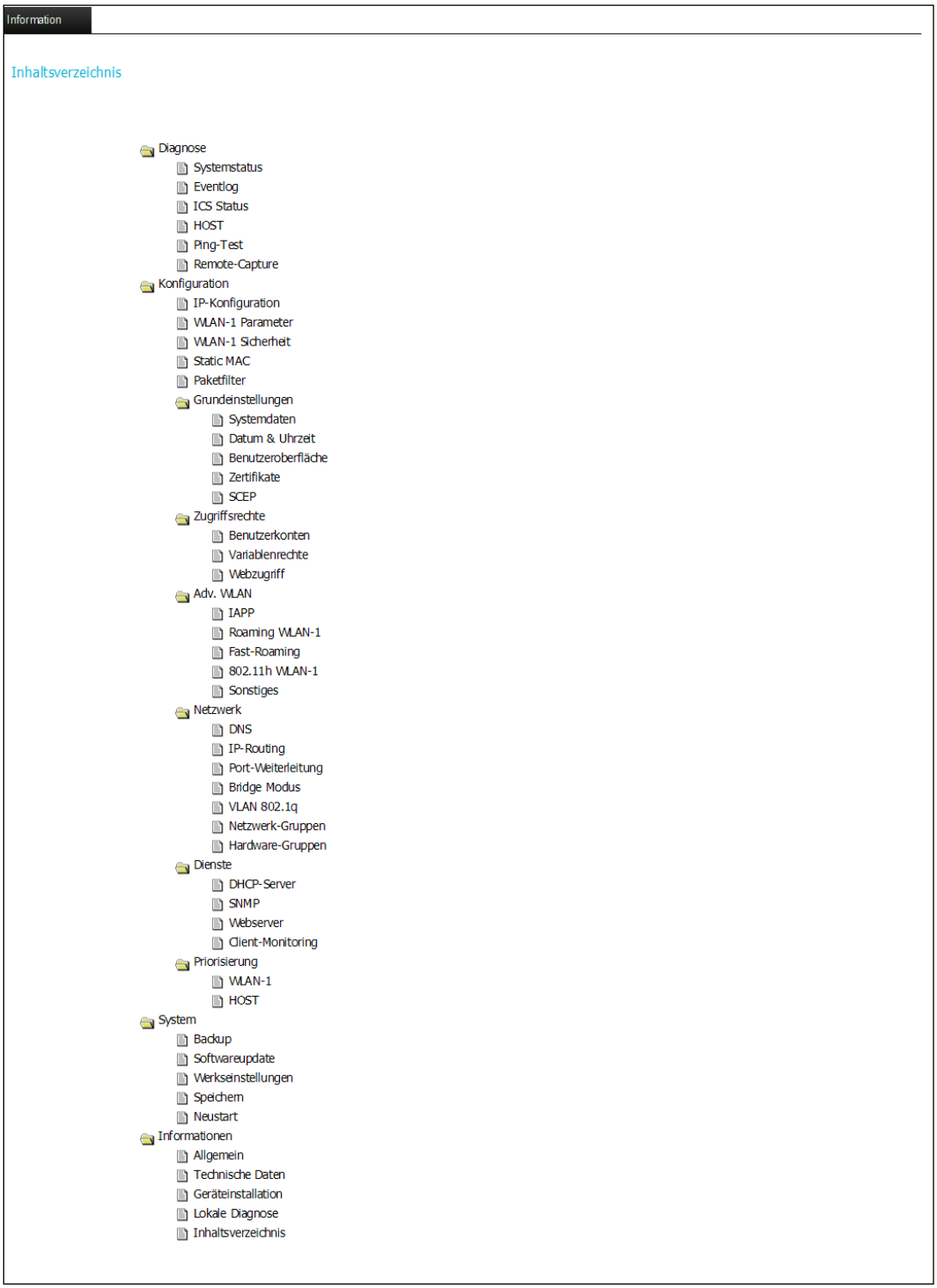
8.6.4 LOKALE DIAGNOSE

Die Lokale Diagnose zeigt das Anzeigeverhalten der LEDs bei verschiedenen Systemaktivitäten an.



8.6.5 INHALTSVERZEICHNIS

Das Inhaltsverzeichnis zeigt das Webinterface als Baumstruktur mit allen Untermenüs zur leichten Navigation an.



9 ZULASSUNGEN

9.1 EUROPAZULASSUNGEN

Hinweis:
Durch länderspezifische Regelungen können Einschränkungen entstehen, welche den Funktionsumfang des Geräts beinträchtigen .

Länder	Kennzeichnung	2,4 - 2,4835 GHz IEEE 802.11b/g	Einschränkungen
Belgien	CE ①	X	The device in the 5150-5350 MHz may only be used indoors. TPC and DFS is mandatory for 5GHz-band.
Deutschland	CE ①	X	
Finnland	CE ①	X	
Griechenland	CE ①	X	
Irland	CE ①	X	Indoor use only restriction in the 5150-5350 MHz band
Lettland	CE ①	X	
Luxemburg	CE ①	X	Only indoor use for the frequency band of 5150 - 5350 MHz. Only mobile applications allowed in the 5 GHz band.RLAN/WLAN used for public service need a generale autorisation from the ILR (Institut Luxembourgeois de Regulation)
Niederlande	CE ①	X	
Polen	CE ①	X	
Schweden	CE ①	X	
Slowenien	CE ①	X	
Tschechien		X	
Zypern	CE ①	X	
Dänemark	CE ①	X	
Estland	CE ①	X	
Frankreich	CE ①	X	
Großbritannien	CE ①	X	

Italien	CE ①	X	
Litauen	CE ①	X	
Malta	CE ①	X	Consequently this equipment may be placed on the local market, subject that a copy of the Declaration of Conformity is submitted to this Authority by the person intending to market the equipment.
Österreich	CE ①	X	
Portugal	CE ①	X	Information: for this type of applications an integral or dedicated antenna is required in the frequency of 5250-5350MHz and 5470-5725MHz DFS and TPC are mandatory If the equipment does not have DFS implemented the use will be limited to the frequency of 5150-5250MHz, with a maximum output power limited of e.i.r.p of 0.25mW/25kHz for each 25kHz.the maximum output power should be in E.I.R.P
Slowakei	CE ①	X	Int the Slovak Republic operation of the wireless LAN equipment is allowed in the frequency band 2400 - 24835 MHz against the conditions laid down in the General authorisation No. VPR-01/2001 (20 dBM EIRP) issued by the Telecommunications Office of the SR. In the frequency band 5150 - 5350 MHz operation of WLAN equipment is allowed against the conditions laid down in the General authorisation No.: VPR-03/2004 (indoor only: 5150 - 5350 with DFS: 200mW EIRP with TPC, 120mW EIRP without TPC; 5150 - 5250 without DFS: 120mW EIRP with TPC, 60mW EIRO without TPC)In the frequency band 5470 - 5725 MHz operation of WLAN equipment is allowed against the conditions laid down in the General authorisation No.: VPR-07/2004 (1W EIRP, DFS + TCP is required)
Spanien	CE ①	X	
Ungarn	CE ①	X	
Schweiz	CE ①	X	

Norwegen	CE ①	X	
Island	CE ①	X	

9.1 KANALLISTEN

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
FCC	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	36	5180	No Outdoor!
	40	5200	No Outdoor!
	44	5220	No Outdoor!
	48	5240	No Outdoor!
	149	5745	
	153	5765	
	157	5785	
	161	5805	
	165	5825	

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Hinweis:
Für den Standard ETSI sind nachfolgend länderspezifische Einstellungen zu beachten!

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
ETSI	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	
	36	5180	No Outdoor!
	40	5200	No Outdoor!
	44	5220	No Outdoor!
	48	5240	No Outdoor!
	52	5260	No Outdoor!, DFS
	56	5280	No Outdoor!, DFS
	60	5300	No Outdoor!, DFS
	64	5320	No Outdoor!, DFS
	100	5500	DFS
	104	5520	DFS
	108	5540	DFS
	112	5560	DFS
	116	5580	DFS
	120	5600	DFS
	124	5620	DFS
	128	5640	DFS
	132	5660	DFS
	136	5680	DFS
	140	5700	DFS

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
Argentinien	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	
	56	5280	DFS
	60	5300	DFS
	64	5320	DFS
	149	5745	
	153	5765	
	157	5785	
	161	5805	
	165	5825	

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
Ägypten	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	
	36	5180	Nur 20MHz Breite!
	40	5200	Nur 20MHz Breite!
	44	5220	Nur 20MHz Breite!
	48	5240	Nur 20MHz Breite!
	52	5260	Nur 20MHz Breite!, DFS
	56	5280	Nur 20MHz Breite!, DFS
	60	5300	Nur 20MHz Breite!, DFS
	64	5320	Nur 20MHz Breite!, DFS

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
Brasilien	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	
	36	5180	
	40	5200	
	44	5220	
	48	5240	
	52	5260	DFS
	56	5280	DFS
	60	5300	DFS
	64	5320	DFS
	100	5500	DFS
	104	5520	DFS
	104	5520	DFS
	108	5540	DFS
	112	5560	DFS
	116	5580	DFS
	120	5600	DFS
	124	5620	DFS
	128	5640	DFS
	132	5660	DFS
	136	5680	DFS
	140	5700	DFS
	149	5745	
	153	5765	

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

	157	5785	
	161	5805	
	165	5825	

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
China	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	
	149	5745	
	153	5765	
	157	5785	
	161	5805	
	165	5825	

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
Russland	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	
	13	2472	

Hinweis:
Für Japan sind im Gerät, abhängig von der jeweiligen Region, genauere Einstellungen vorzunehmen. Beispielhaft ist die Region 1 abgebildet.

Land/Zertifizierug	Kanal	Frequenz (MHz)	Einschränkungen
Japan1	1	2412	
	2	2417	
	3	2422	
	4	2427	
	5	2432	
	6	2437	
	7	2442	
	8	2447	
	9	2452	
	10	2457	
	11	2462	
	12	2467	Nur 20MHz Breite!
	13	2472	Nur 20MHz Breite!
	34	5170	
	38	5190	
	42	5210	
	48	5230	

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

9.2 5 GHz DFS Reglementierung nach ETSI EN 301 893 V1.4.1 innerhalb der EU

Indoor Kanäle:

Kanalnummer [1)]	Frequenz (MHz)	Max. zul. Abstrahlleistung mit TPC
36	5.180	23 dBm
40	5.200	23 dBm
44	5.220	23 dBm
48	5.240	23 dBm

1) Können manuell konfiguriert werden, DFS ist nicht aktiviert. TPC ist bei ads-tec Geräten auf 5 GHz immer aktiv.

Outdoor Kanäle:

Kanalnummer[2)]	Frequenz (MHz)	Max. Abstrahlleistung mit TPC [4)]	DFS Wartezeit[3)]
52	5.260	23 dBm	1 min.
56	5.280	23 dBm	1 min
60	5.300	23 dBm	1 min
64	5.320	23 dBm	1 min
100	5.500	30 dBm	1 min
104	5.520	30 dBm	1 min
108	5.540	30 dBm	1 min
112	5.560	30 dBm	1 min
116	5.580	30 dBm	1 min
120	5.600	30 dBm	10 min[5)]
124	5.620	30 dBm	10 min[5)]
128	5.640	30 dBm	10 min[5)]
132	5.660	30 dBm	1 min
136	5.680	30 dBm	1 min
140	5.700	30 dBm	1 min

2)Können nur automatisch ausgewählt werden. DFS ist immer aktiviert. TPC ist bei ads-tec Geräten auf 5 GHz immer aktiv.

[3])Die DFS Wartezeit wird beim Einschalten sowie bei Kanalwechsel durch Radardetektion aktiv.

4)Access Clients dürfen ohne eigenes DFS arbeiten, wenn Sie mit TPC bei einer maximalen Abstrahlleistung von 23 dBm bleiben. Bei ads-tec Access Clients kann zusätzlich DFS aktiviert werden, sodass wie bei den APs eine Abstrahlleistung von 30 dBm mit TPC zulässig ist.

5)5.6 GHz Wetterradar-Kanäle müssen bei ads-tec Access Points separat aktiviert werden.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

9.3 FCC-APPROVAL

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Warning:

Changes or modifications made to this equipment not expressly approved by ads-tec GmbH may void the FCC authorization operate this equipment.

Special Note:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled

environment. This equipment should be installed and operated with minimum distance of 20cmbetween the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

9.4 RICHTLINIEN

RAP 1120, RAP 1121, RAP 1220,

RAP 1220, RAP 1221, RAC 1110, RAC 1111, RAC 1510, RAC1511

stimmen in der von ads-tec GmbH in Verkehr gebrachten Ausführung mit den Vorschriften der folgenden europäischen Richtlinie überein:

99/5/EG

Richtlinie des europäischen Parlaments und des Rates zur Angleichung derRechtsvorschriften der Mitgliedstaaten über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.

Die Konformität mit den grundlegenden Anforderungen der Richtlinie wird nachgewiesen durch die Einhaltung folgender Normen:

EN 60950

Sicherheit von Einrichtungen der Informationstechnik

EN 301489-1

Elektromagnetische Verträglichkeit für Funkeinrichtungen und -dienste

EN 301489-17

Spezifische Bedingungen für Breitband-Datenübertragungssysteme und für Einrichtungen in lokalen Hochleistungs-Funknetzen (HIPERLAN)

EN 300328

Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten

EN 301893

Breitband-Funkzugangsnetze (BRAN) - 5-GHz-Hochleistungs-RLAN

EN 50371

Übereinstimmung von elektronischen und elektrischen Geräten kleiner Leistung

mit den Basisgrenzwerten für die Sicherheit von Personen in elektromagnetischen

Feldern (10 MHz bis 300 GHz)

1999/519/EC

Empfehlung des Rates zur Begrenzung der Exposition der Bevölkerung gegenüber

elektromagnetischen Feldern (0 Hz — 300 GHz)

An das System angeschlossene Geräte müssen die relevanten Sicherheitsbestimmungen erfüllen.

Die EG-Konformitätserklärung wird gemäß den obengenannten EG- Richtlinien für

die zuständigen Behörden zur Verfügung gehalten bei:

ads-tec GmbH

Raiffeisenstraße 14

70771 Leinfelden-Echterdingen / Oberaichen

Diese Erklärung bescheinigt die Übereinstimmung mit den genannten Richtlinien,

ist jedoch keine Zusicherung von Eigenschaften.

10 TECHNISCHE DETAILS

10.1 VARIANTEN

		RAP – Rugged Access Point											
		RAP1000 Serie											
		RAP 1110	RAP 1111	RAP 1210	RAP 1211	RAP 1120	RAP 1121	RAP 1220	RAP 1221	RAP 1510	RAP 1511	RAP 1520	RAP 1521
Funkmodule	1 WLAN Modul	x	x	x	x					x	x		
	2 WLAN Module					x	x	x	x			x	x
Ports	1x Cu-RJ45 Port	x	x			x	x			x	x	x	x
	4x Cu-RJ45 Port (switch)									x	x	x	x
	1x Glasfaser Ethernet Port			x	x			x	x				
Spannungs-versorgung	24 V DC	x	x	x	x	x	x	x	x	x	x	x	x
	110/230 V AC integriert		x		x		x		x		x		x
	Redundant e Spannungsversorgung	x	x		x	x	x		x	x	x	x	x
Client Modus	RAP incl. Client - Modus	x	x	x	x	x	x	x	x	x	x	x	x
	Seamless Roaming Client*					x	x	x	x			x	x

		RAC – Rugged Access Client					
		RAC1000 series				RAC2000 series	
		RAC 1120	RAC 1121	RAC 1220	RAC 1221	RAC 2110	RAC 2120
Funkmodule	1 WLAN Modul					x	
	2 WLAN Module	x	x	x	x		x
Ports	1x Cu-RJ45 Port	x	x			x	x
	4x Cu-RJ45 Port (Switch)						
	1x Ethernet port			x	x		
Spannungsversorgung	24 V DC	x	x	x	x	x**	x**
	110/230 V AC integriert		x		x		
	Redundante Spannungsversorgung	x	x		x		
Client Modus	RAP incl. Client Modus						
	Seamless Roaming Client*	x	x	x	x		x

* Seamless Roaming Clients: Von Access Point zu Access Point ohne jeglichen Paketverlust oder Unterbrechung der Datenverbindung
**12 – 24V

10.2 DATENÜBERTRAGUNG ETHERNET

HOST Ethernet Stecker	RJ45 oder LWL (MTRJ)
Übertragungsrate Ethernet	10/100 Mbit/s
Optional Switch	4x RJ45 mit 10/100 Mbit/s

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

10.3 Funk Eigenschaften

Frequenzbereich	2,412 bis 2,483 GHz 5,15 bis 5,34 GHz 5,47 bis 5,725 GHz
Funkkanäle	13 bei 802.11b/g 19 bei 802.11a
Übertragungsbandbreite	802.11b (11 Mbit/s) 802.11g (54 Mbit/s) 802.11a (54 Mbit/s) 802.11h (54 Mbit/s)
Sendeleistung max.	20 dBM EIRP, 17dBm am R-SMA Anschluss
Modulationstechnik	802.11b: DSSS 802.11g: OFDM 802.11a/h: OFDM
Impedanz	50 Ohm
Polarität	Vertikal / Horizontal
Antennen	2x R-SMA Anschlüsse je Funkmodul

10.4 Energieversorgung

Spannungsversorgung	24 V DC 110/230 V AC PoE 48VDC über RJ45
Stromaufnahme	max. 500mA

10.5 Konfiguration

Software	WEB-based Interface (deutsch/englisch) über http oder https, Passwort geschützt.

10.6 Allgemeine Daten

Außenmaße ohne Antenne	250 mm x 160 mm x 65 mm (B x H x T)
Außenmaße mit 2 Antennen	425 mm x 335 mm x 65 mm (B x H x T)
Außenmaße mit 4 Antennen	600 mm x 335 mm x 65 mm (B x H x T)
Gewicht	ca. 1 kg
Schutzart	IP65

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

11 SERVICE UND SUPPORT

Die Firma ads-tec und Ihre Partnerfirmen bieten Ihren Kunden einen umfassenden Service und Support, die eine schnelle und kompetente Unterstützung bei allen Fragen zu ads-tec Produkten und Baugruppen zur Verfügung stellen.

Da die Geräte der Firma ads-tec auch von Partnerfirmen eingesetzt werden, können diese Geräte kundenspezifisch konfiguriert sein. Entstehen Fragen zu diesen speziellen Konfigurationen und Softwareinstallationen, so können diese nur vom Anlagenhersteller beantwortet werden.

Bei Geräten, die nicht direkt bei ads-tec gekauft wurden, wird kein Support übernommen. In diesem Fall wird der Support von unserer Partnerfirma übernommen.

11.1 ADS-TEC SUPPORT

Das Support Team von ads-tec steht für Direktkunden von Montag bis Freitag von 8:30 bis 17:00 Uhr unter der unten genannten Telefonnummer zur Verfügung:

Tel: +49 7022 2522-202
Fax: +49 7022 2522-2602
E-Mail: support@ads-tec.de

Alternativ können Sie auf unserer Webseite www.ads-tec.de ein Supportformular zur Kontaktierung verwenden. Unser Support wird sich dann schnellstmöglich mit Ihnen in Verbindung setzen.

11.2 FIRMENADRESSE

ads-tec GmbH
Heinrich-Hertz-Str.1
72622 Nürtingen
Germany

Tel: +49 7022 2522-0
Fax: +49 7022 2522-400
E-Mail: mailbox@ads-tec.de
Home: www.ads-tec.de

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

12 ANWENDUNGSBEISPIELE

12.1 PRIORISIERUNG

ALLGEMEIN

Heutzutage werden sehr viele unterschiedliche Arten von Daten über Kommunikationsnetzwerke übermittelt und auch die Datenmenge nimmt immer weiter zu. Mit Hilfe einer Priorisierung können den unterschiedlichen Datenarten auch unterschiedliche große Übertragungsraten zugeordnet werden, sodass sich ein Download nicht negativ auf eine VoIP-Verbindung auswirkt. Im Gegensatz zu den drahtgebundenen Netzwerken wird ein WLAN durch einen kleineren Datendurchsatz eingeschränkt. Hier ist eine Priorisierung also besonders ratsam.

ERWEITERUNGEN AUS 802.11E

Die RAP/RAC Geräte von ads-tec implementieren zusätzlich zur Benutzergesteuerten Priorisierung auch die QoS Erweiterungen aus dem 802.11e Standard. Diese Erweiterungen sind permanent aktiv. In 802.11e werden 4 Klassen definiert, wobei Voice die höchste Priorität hat:

- Best Effort
- Background
- Video
- Voice

Für die Klassifizierung wird das Type Of Service Feld nach folgender Tabelle ausgewertet:

IP ToS	802.11e Klasse
0x20	Background
0x40	
0x80	Video
0xA0	
0xC0	Voice
0xE0	
0x88	
0xB8	
restliche	Best Effort

Wenn nun mehrere Datenverbindungen gleichzeitig aktiv sind, kann eine VoIP Verbindung durch setzen des Type Of Service Feldes (zum Bsp: auf 0xC0) bevorzugt über das WLAN übertragen werden.

Hinweis:
Die 802.11e Priorisierung wird nur auf ausgehende Pakete angewandt!

Die 802.11e Erweiterungen sind immer aktiv und somit auch ohne Konfiguration verfügbar. Die benötigten Einstellungen zur Benutzergesteuerten Priorisierung werden im Folgenden erläutert.

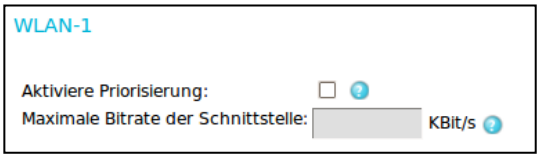
© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

KONFIGURATION

Unter dem Menüpunkt „**Konfiguration → Priorisierung**“ können alle Schnittstellen getrennt konfiguriert werden.

AKTIVIERUNG

Durch setzen des Häkchens „Aktiviere Priorisierung“ und der Angabe einer maximalen Bitrate wird die Priorisierung für eine Schnittstelle gestartet. Für diesen Fall, also noch keine Klassen definiert, wird das Gerät alle Datenarten bis zu der gewählten Bitrate weiterleiten und die Überschüssigen verwerfen.

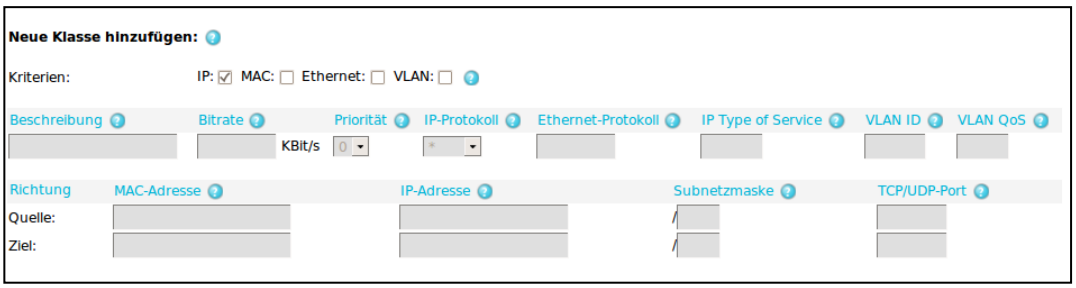


Hinweis:

Die Priorisierung wird nur auf ausgehende Pakete angewandt!

KLASSEN HINZUFÜGEN

Wie bereits erwähnt wird die eigentliche Priorisierung in Klassen eingeteilt. Dabei werden die unterschiedlichen Datenarten einer oder mehreren Klassen zugeordnet. Die einzelnen Klassen selbst sind in einer Tabelle abgelegt. Sie können über die bekannten Knöpfe gelöscht oder in ihrer Position verändert werden.



Hinweis:
Die Position spielt für die spätere Priorisierung eine wichtige Rolle, da für jedes Datenpaket die einzelnen Klassen sequentiell abgearbeitet werden und beim ersten Treffer die Klasse verwendet wird

KLASSEN HINZUFÜGEN

Eine Klasse enthält Kriterien nach denen die Datenpakete analysiert und eingeordnet werden:

- IP: für IP-Pakete
- Ethernet: für Ethernet Frames
- VLAN: für VLAN-Pakete

Zusätzlich können zu diesen 3 Kriterien noch die MAC-Adressen als Kriterium mit aufgenommen werden.

Nun kann mit Hilfe folgender Kriterien, noch weiter unterschieden werden:

IP-Protokoll	Das im IP-Paket enthaltene Transport Protokoll: TCP/UDP/ICMP oder * für alle.
Ethernet Protokoll	Die Protokollnummer in Hexadezimal Schreibweise. Erlaubt sind Werte zwischen 0x0600 – 0xFFFF.
IP Type of Service	Das Internet Protokoll spezifisiert mit diesem Feld selbst eine Priorisierung, welche hier ausgewertet und als Kriterium herangezogen werden kann.
VLAN ID	Die eindeutige Kennnummer eines VLANs. Wird 0 gewählt, so wird das VLAN QoS ausgewertet.
VLAN QoS	Werte zwischen 0-7, die die Priorisierung angeben. Wird nur auswertet wenn die VLAN ID gleich 0 ist.
MAC-Adressen	Ziel und Quell MAC-Adresse.
IP-Adressen	Ziel und Quell IP-Adresse mit Netzmaske.
Portnummer	Die Portnummer, falls TCP oder UDP ausgewählt wurde.

Zu jeder Klasse muss dann ein Name sowie die Bitrate und die Priorität angegeben werden. Dabei muss beachtet werden, dass die Summe alle Klassenbitraten nicht die Bitrate der Schnittstelle überschreitet. Für die Priorität werden Werte zwischen 0 (Hoch) und 7 (Niedrig) vergeben.

Wird für eine Datenart keine Klasse gefunden so wird automatisch die Priorität 7 vergeben und die restliche Bitrate verwendet.

Hinweis:
Werden alle Felder für die Kriterien leer gelassen und diese Regel ans Ende der Tabelle eingefügt, so kann das Verhalten angepasst werden, dass normalerweise auf nicht klassifizierte Datenarten angewandt wird.

BEISPIEL

In dem obigen Beispiel wurde die Maximale Bitrate der Schnittstelle auf 5Mbit/s gesetzt. Diese Bitrate teilen sich 3 Klassen. Die erste Klasse mit einer niedrigen Priorität und nur 0.5Mbit/s Bitrate beschreibt normale HTTP-Verbindungen. Die zweite Klasse ist für VoIP Verbindungen mit 3.5Mbit/s und der höchsten Priorität reserviert. Die dritte Klasse, ist die Default Klasse (nicht konfiguriert), in die der restliche Datenverkehr fällt. Dieser bekommt die noch restlichen 1Mbit/s zugeteilt.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

DEAKTIVIEREN DER PRIORISIERUNG

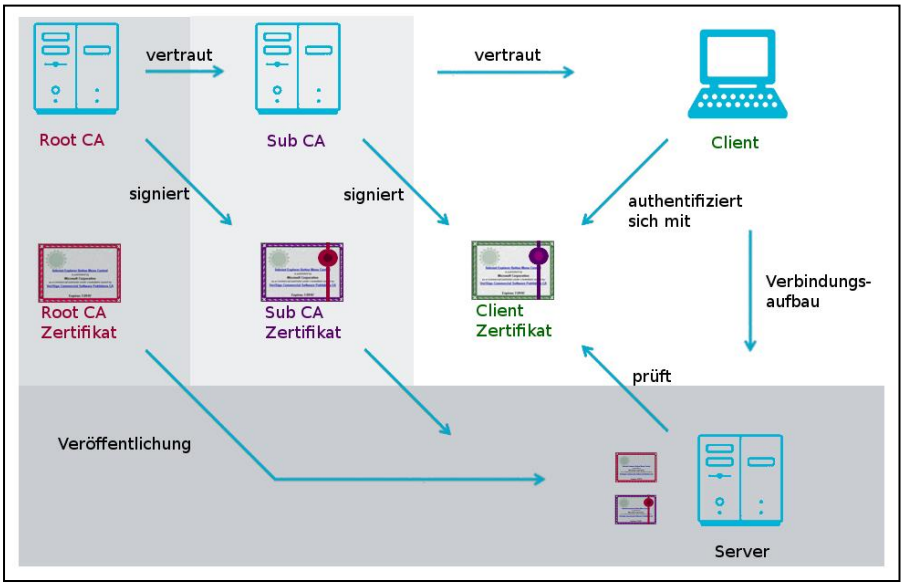
Unter dem Menüpunkt „**Konfiguration → Priorisierung**“ können alle Schnittstellen deaktiviert werden. Dazu den Haken von „**Aktiviere Priorisierung**“ entfernen.

12.2 ZERTIFIKATE

ALLGEMEIN

Zertifikate dienen zur Authentifizierung eines Computers oder Benutzers und zur Verschlüsselung einer Verbindung (z.B. OpenVPN, IPsec, Webseite). Um ein Zertifikat zu diesem Zweck verwenden zu können, muss es von einer Zertifizierungsstelle (CA) signiert worden sein. Zur Authentifizierung wird das Zertifikat der Gegenstelle mit dem Zertifikat der CA geprüft. Ist die Signatur gültig und die CA vertrauenswürdig, dann gilt die Gegenstelle als authentifiziert. Ein CA-Zertifikat wird Root-Zertifikat genannt, wenn es die Grundlage der Authentifizierung bildet und selbst nicht durch eine andere Instanz signiert wurde (self-signed Certificate). Eine solche Root-CA kann dazu genutzt werden, untergeordnete CA-Zertifikate zu signieren. So entsteht eine Vertrauens-Kette („Chain-of-trust“) deren Grundlage das Root-Zertifikat ist.

Um ein Zertifikat zu verifizieren, das durch eine CA signiert wurde, die keine Root-CA ist, müssen die Zertifikate aller übergeordneten CAs zur Verfügung stehen.



Beispiel: Eine Root-CA (ads-tec Root-CA) signiert eine untergeordnete Sub-CA (ads-tec ST-CA), die wiederum ein Client-Zertifikat für eine OpenVPN Verbindung signiert. Um das Client-Zertifikat zu prüfen, muss sowohl das Zertifikat von „ads-tec ST-CA“ als auch das von „ads-tec Root-CA“ auf dem System vorhanden sein.

ads-tec Geräte aus dem Bereich IT Infrastructure unterstützen solche mehrstufige CA-Hierarchien. Sofern alle CA-Zertifikate der Hierarchie vorliegen, werden bei den Zertifikats-basierten Diensten (z.B. OpenVPN, IPsec, Radius) immer die vollständigen Pfade der Hierarchie geprüft. Sollte sich dabei ein CA-Zertifikat der Kette als ungültig erweisen, so gilt dies auch für alle untergeordneten Zertifikate.

Um den Missbrauch verlorengegangener oder kompromitierter Zertifikate zu unterbinden, kann von einer CA eine Sperrliste (CRL) eingerichtet werden. Zertifikate auf dieser Liste gelten dann trotz korrekter Signatur als ungültig.

Hinweis:

Bei dieser Art der Authentifizierung wird überprüft, ob ein Zertifikat von einer bestimmten Zertifizierungsstelle herausgegeben (bzw. signiert) wurde. Die Sicherheit basiert also auf dem Vertrauen in die Zertifizierungsstelle, d.h. dem Vertrauen darauf, dass diese das Zertifikat nur zu dem angegebenen Zweck ausgegeben (bzw. signiert) hat (z.B. zur Authentifizierung einer bestimmten Webseite)!

ERSTELLEN VON ZERTIFIKATEN MIT OPENSSL

CA-Zertifikate und damit signierte Zertifikate können mit OpenSSL über die Eingabeaufforderung erstellt werden. OpenSSL für Windows kann von http://www.openssl.org/related/binaries.html heruntergeladen werden. Anleitungen finden sich zum Beispiel auf:

- http://www.online-tutorials.net/security/openvpn-tutorial/tutorials-t-69-209.html
- http://www.madboa.com/geek/openssl/

Hinweis:

Die Beispielzertifikate dienen der Veranschaulichung und dürfen auf keinen Fall für eine echte Authentifizierung verwendet werden!

Die Zertifikate sind ab dem Zeitpunkt der Erstellung gültig - das Datum auf dem erzeugenden Rechner muss also korrekt sein.

Eine Zertifikats-Infrastruktur kann auch mit Hilfe der Microsoft Windows Server 2000/2003 PKI erstellt werden. Ein Einstiegspunkt ist: http://www.microsoft.com/pki.

Die Identitätsangaben (Country Name, usw.) müssen gemacht werden, damit jedes Zertifikat eindeutig ist! Zwei unterschiedliche Zertifikate dürfen nicht genau die gleichen Angaben verwenden. Es muss mindestens ein Feld unterschiedlich sein (zum Beispiel der Common Name).

Zertifikatsverwaltung mit OpenSSL ist durch die Bedienung per Windows Kommandozeile etwas mühsam, weshalb wir für Anwendungsfälle im kleineren Maßstab die Verwendung eines graphischen Frontends empfehlen. Daher wird im nächsten Kapitel die Verwendung der freien Software „XCA“ erklärt.

ERSTELLEN VON ZERTIFIKATEN MIT XCA

Schlüsselverwaltung mit XCA für OpenVPN

Dieses Kapitel erläutert Ihnen die Erstellung und Bedienung von CA, Server- und Client-Zertifikaten mit XCA – speziell für die Verwendung mit OpenVPN.

Einleitung:

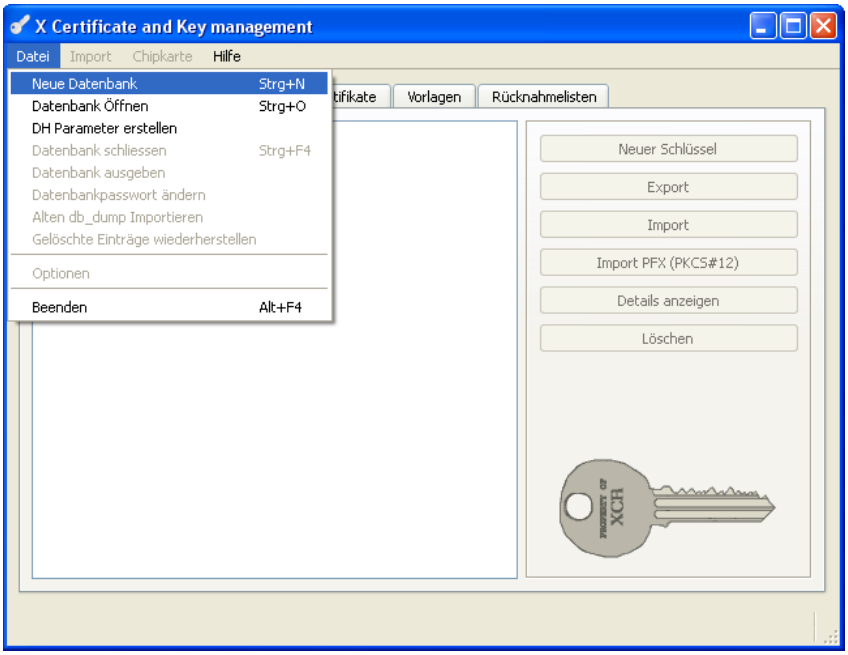
Für das Zertifikate-Management ist XCA ein sehr nützliches und vielfältiges Werkzeug. Zunächst kann die Vielfalt an Möglichkeiten verwirrend wirken, wenn man doch „nur“ ein paar Zertifikate für OpenVPN erstellen möchte. Die Grundlage für dieses Dokument ist die XCA Version 0.9.0.

Hilfreiche Links:

Zusätzliche Tipps und Hinweise finden Sie unter: http://XCA.sourceforge.net/

Download der aktuellen XCA Version unter dem folgenden Link : http://sourceforge.net/projects/XCA/

Bitte installieren Sie das Programm und richten es mit den Standardeinstellungen grundlegend ein. Nach dem ersten Programmstart erstellen Sie sich eine neue Datenbank:

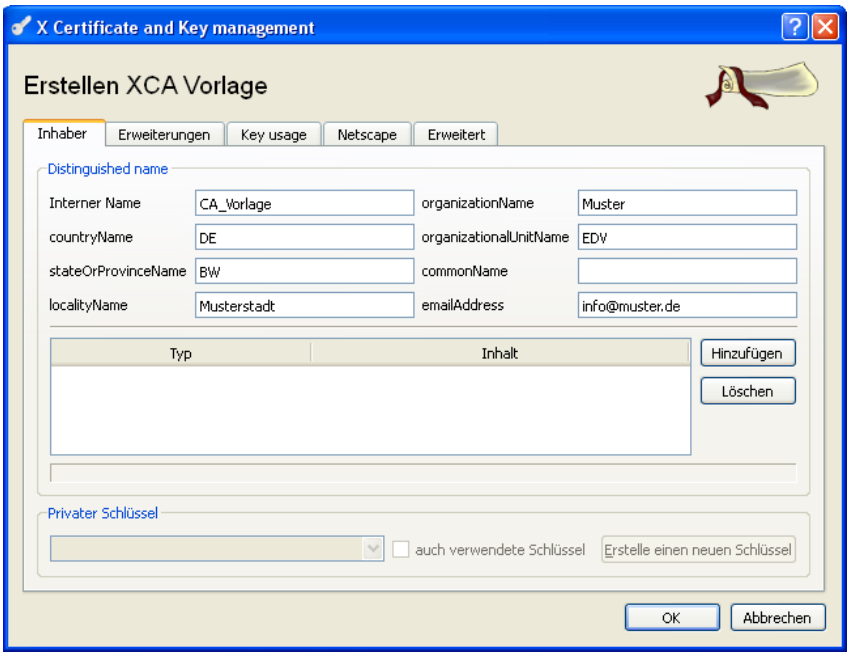


Verwenden Sie einen plausiblen Namen wie z.B. “**CA_Projektname**”. Diese Datenbank muss mit einem Passwort verschlüsselt werden: Heben Sie das Passwort gut auf!

Um die Bedienung von XCA gleich zu Beginn zu vereinfachen, sollten Sie sich vorab Vorlagen für die 3 Standard-Arbeitsschritte erstellen.

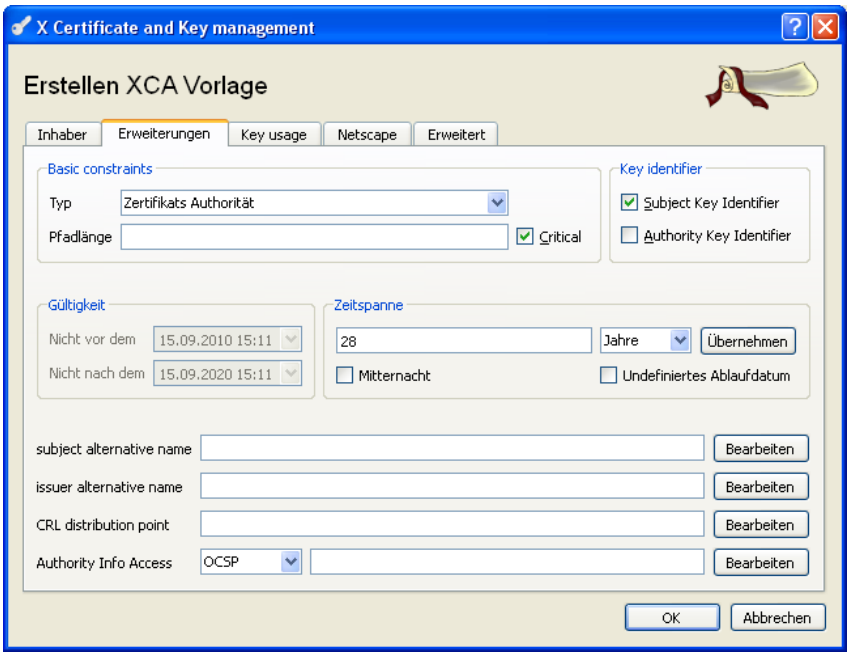
Unter dem Reiter “**Vorlagen**” wählen Sie “**Neue Vorlage**” aus und im folgenden Pop-up Fenster “**CA**”.

Tragen Sie “**CA_Vorlage**” als „**Interner Name**“ für die neue CA-Vorlage ein. Füllen Sie alle Felder aus, außer das Feld “**commonName**”. Dieses bleibt leer.



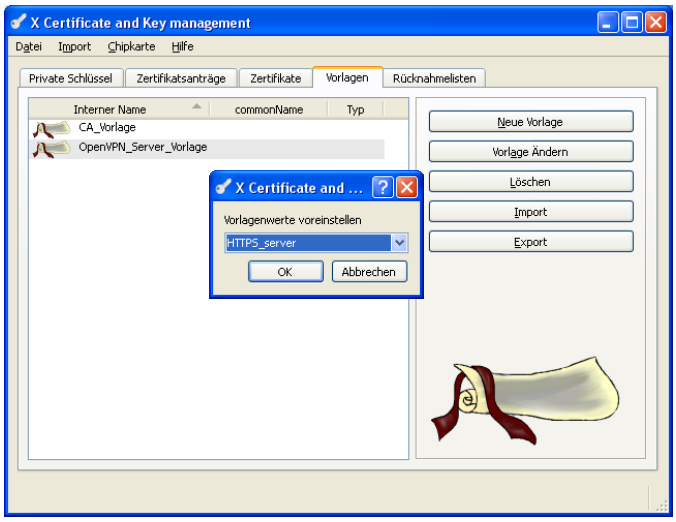
Unter dem nächsten Reiter "**Erweiterungen**" kann die Standard-Gültigkeitsdauer der Zertifikate eingestellt werden.

In der Regel empfiehlt es sich eine längere Zeitspanne zu wählen.



Wenn Sie nun auf „**OK**" klicken, sollten Sie die Meldung bekommen, dass Sie Ihre CA-Vorlage erfolgreich erstellt haben.

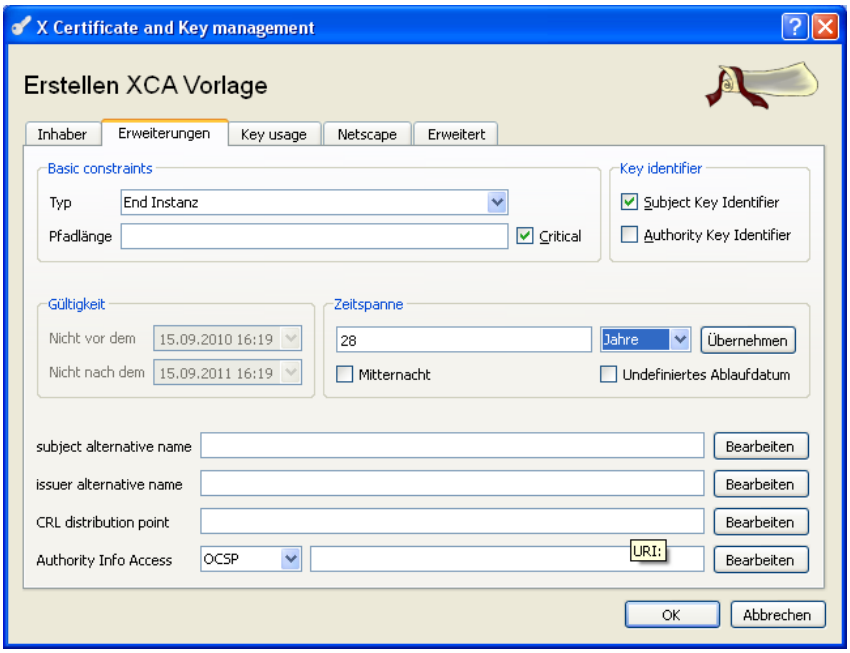
Wiederholen Sie alle bisherigen Schritte, wählen nun aber „**HTTPS_server**" als Vorlage aus.



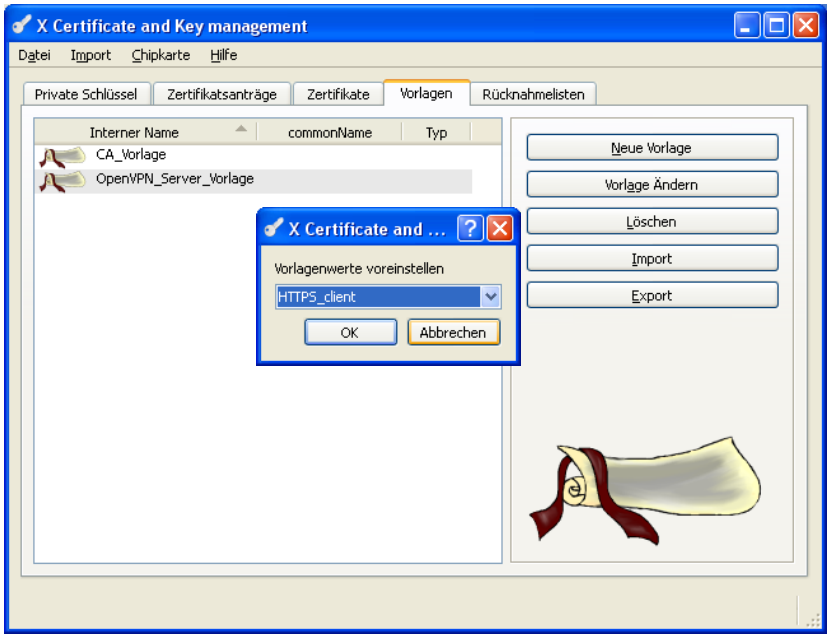
Als “**Interner Name**” empfiehlt sich "**OpenVPN_Server_Vorlage**“. Alle anderen Werte sollten wie bei der CA-Vorlage bleiben.

Besondere Aufmerksamkeit sollten Sie der Gültigkeitsdauer des Zertifikates beimessen. Unter Umständen kann es sinnvoll sein Zertifikate nach einem gewissen Zeitraum zu erneuern und somit kürzere Gültigkeitsdauer zu wählen.

Ansonsten sollte eine längere Zeitspanne gewählt werden:

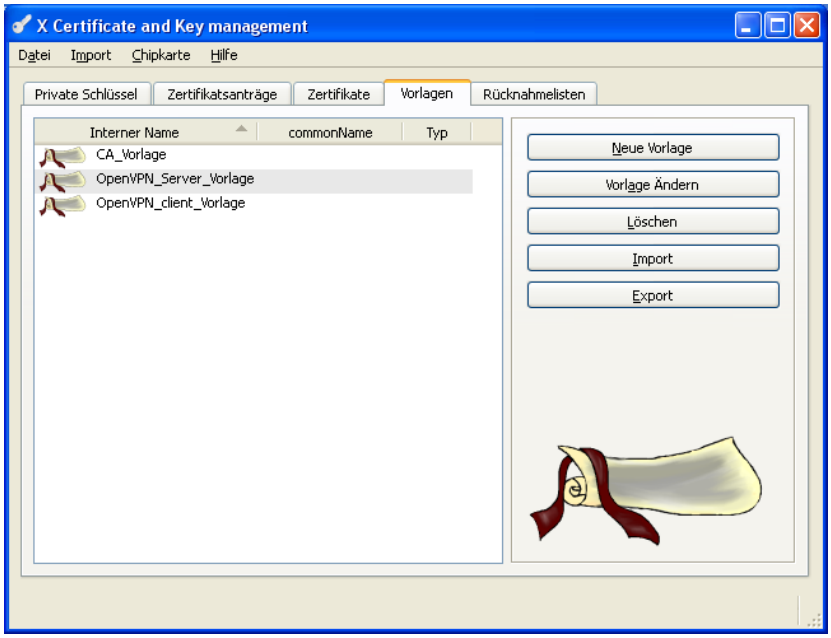


Als Drittes und Letztes wird die Vorlage “**HTTPS_client**” erzeugt.



Als „**Interner Name**“ empfiehlt sich beispielsweise „**OpenVPN_client_Vorlage**“. Ansonsten wählen Sie wieder die gleichen Werte wie bei der Server- und der CA-Vorlage.

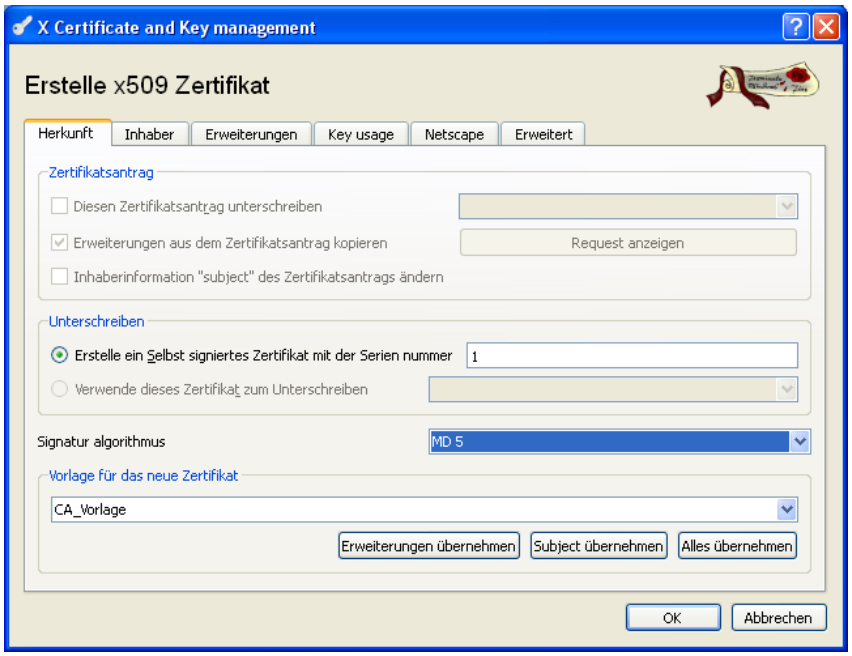
Nun sollten Sie die folgenden drei Vorlagen erstellt haben:



ERSTELLEN EINER CA

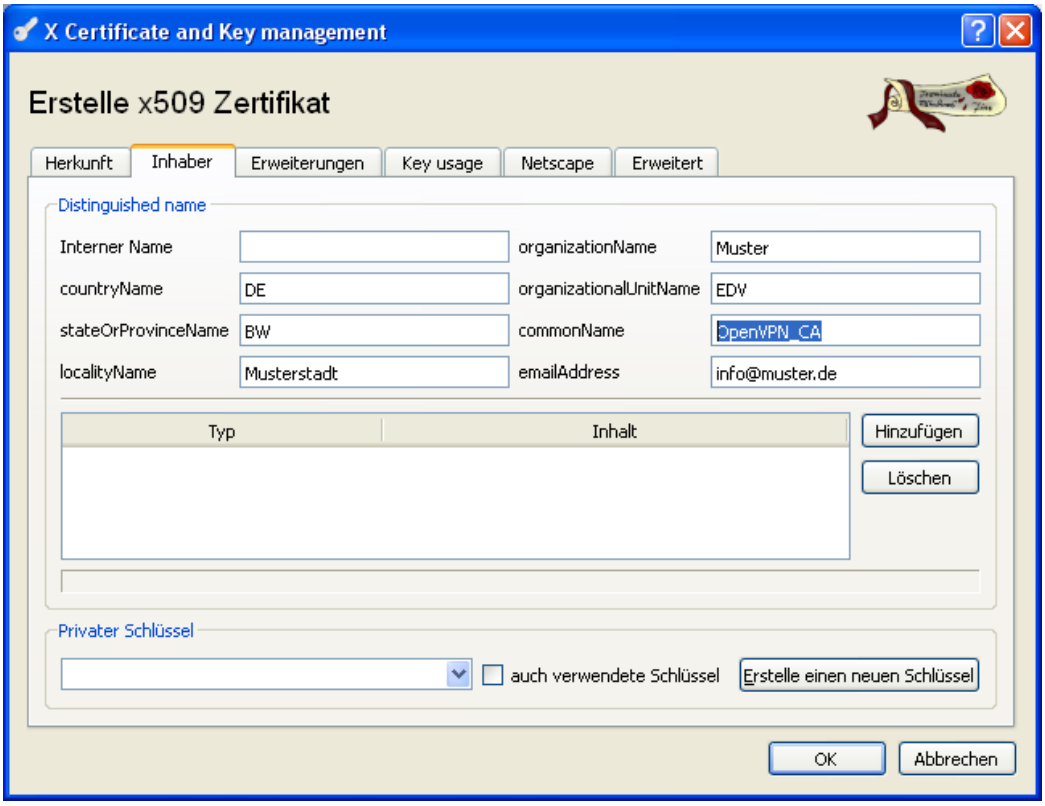
Nun kann mit der Erstellung der benötigten Dateien begonnen werden. Zur Erstellung einer CA können Sie nun die zuvor erstellte CA-Vorlage nutzen. Wählen Sie den Reiter „**Zertifikate**“ und dann „**Neues Zertifikat**“ aus. In dem neuen Fenster unter dem Reiter „**Herkunft**“, wählen Sie nun unten ihre CA-Vorlage („CA_Vorlage“) aus.

Unter “**Signatur Algorithmus**” wechseln Sie zu **'MD5'**. **Vergessen Sie nicht mit „Alles übernehmen“ Ihre Einstellungen zu bestätigen.**

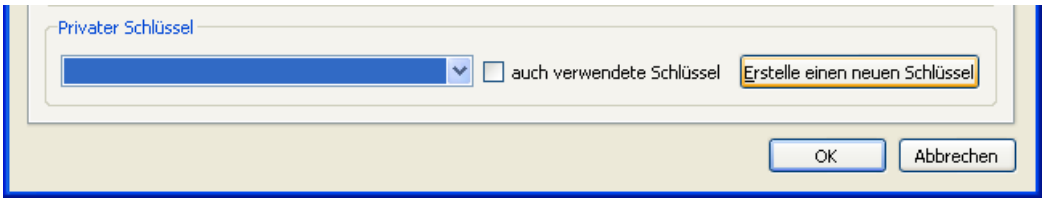


In dem nächsten Reiter “**Inhaber**” geben Sie jetzt unter “**commonName**” einen Namen wie z.B. OpenVPN_CA ein.

Alle anderen Felder sollten aus ihrer Vorlage bereits automatisch befüllt worden sein.

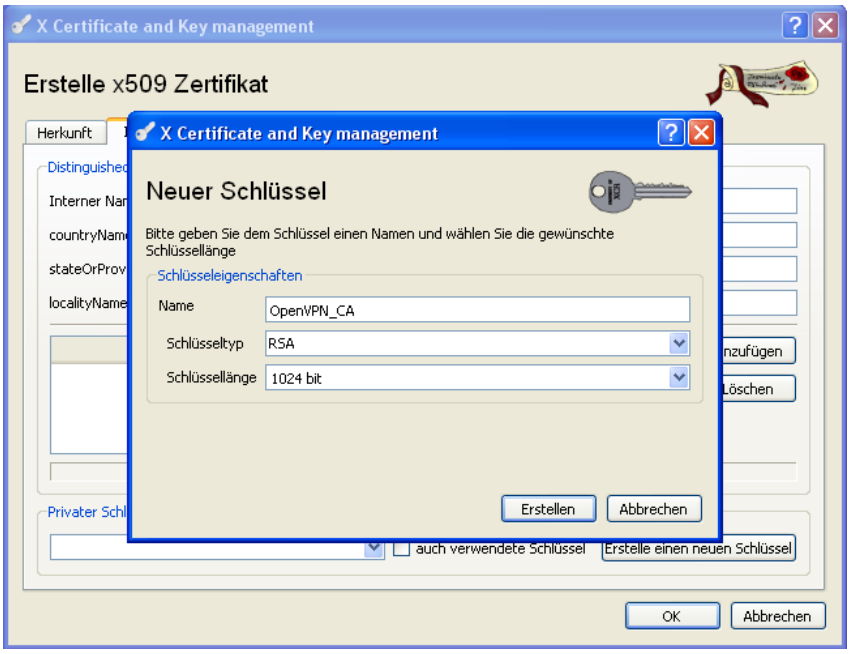


Klicken Sie danach auf “**Erstelle einen neuen Schlüssel**”. Am besten verwenden Sie hier den selben Namen wie bereits unter „**commonName**“. D.h. in unserem Beispiel: „**OpenVPN_CA**“.

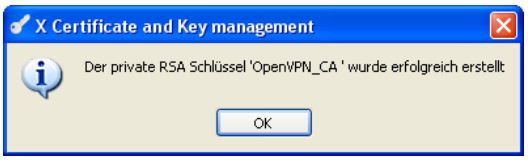


Die Schlüssellänge sollten Sie von Ihrem Sicherheitsbedürfnis abhängig machen. Beachten Sie aber, dass hohe Schlüssellängen die VPN Geschwindigkeit verringern und die Ladezeiten des Systems sowie des Gerätes erhöhen.

In der Regel ist „**2048 bit“** ein guter Wert, der zugleich auch eine hohe Sicherheit bietet.

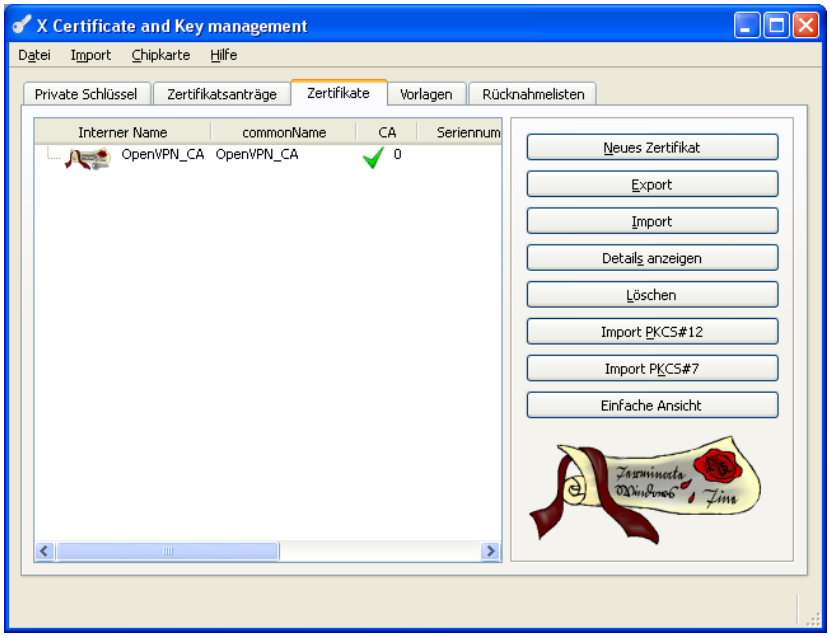


Klicken Sie nun auf „**Erstellen**“. Nun sollte die folgende Meldung erscheinen:



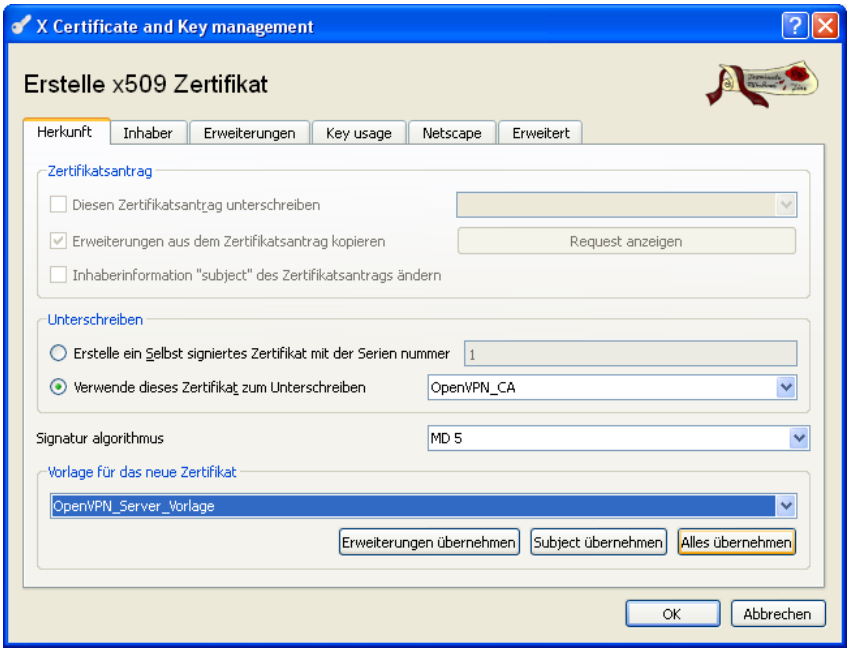
ERSTELLEN EINES SERVER-ZERTIFIKATES

Wählen Sie erneut “**Neues Zertifikat**”.



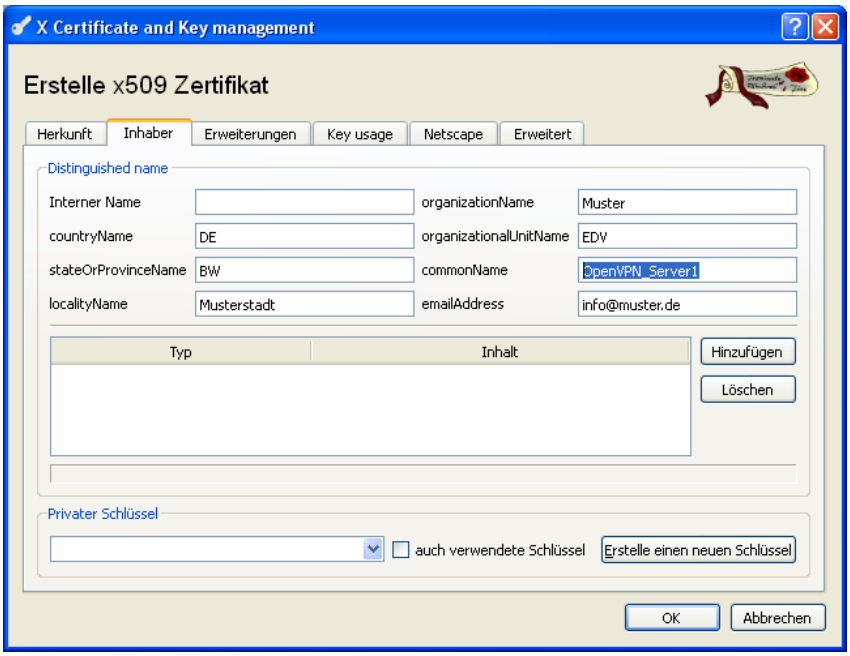
Als „**Signatur Algorithmus**“ wählen Sie **'MD5'**. Unter “**Unterschreiben**” wechseln Sie auf “**Verwende dieses Zertifikat zum Unterschreiben**” und wählen Sie die gerade erstellte CA aus.

Als Vorlage dient diesmal die zu Beginn erstellte Server-Vorlage. Vergessen Sie nicht auf **„Alles Übernehmen“** zu klicken!


X Certificate and Key management
Erstelle x509 Zertifikat
Herkunft Inhaber Erweiterungen Key usage Netscape Erweitert
Zertifikatsantrag
Diesen Zertifikatsantrag unterschreiben
Erweiterungen aus dem Zertifikatsantrag kopieren
Request anzeigen
Inhaberinformation "subject" des Zertifikatsantrags ändern
Unterschreiben
Erstelle ein Selbst signiertes Zertifikat mit der Serien nummer 1
Verwende dieses Zertifikat zum Unterschreiben OpenVPN_CA
Signatur algorithmus MD 5
Vorlage für das neue Zertifikat
OpenVPN_Server_Vorlage
Erweiterungen übernehmen Subject übernehmen Alles übernehmen
OK Abbrechen

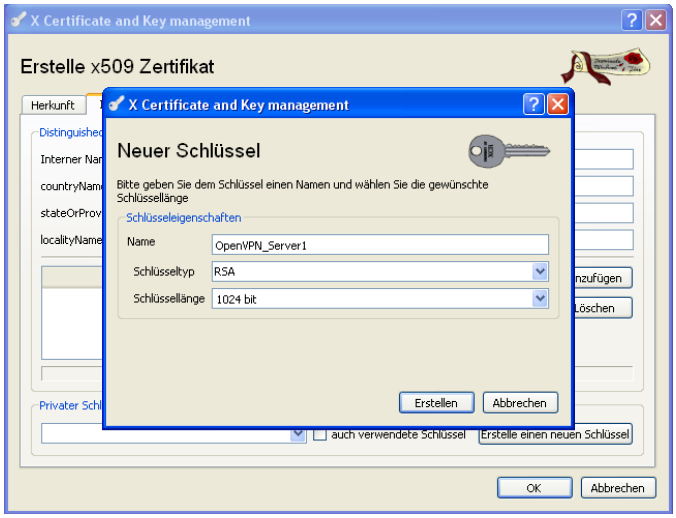
Wechseln Sie nun wieder zum Reiter “**Inhaber**” und geben Sie einen Namen unter “**commonName**” ein, beispielsweise: "**OpenVPN_Server1**".

Alle anderen Felder sollten aus der Vorlage automatisch übernommen worden sein.



Sie müssen nur noch einen neuen Schlüssel für dieses Zertifikat erstellen.

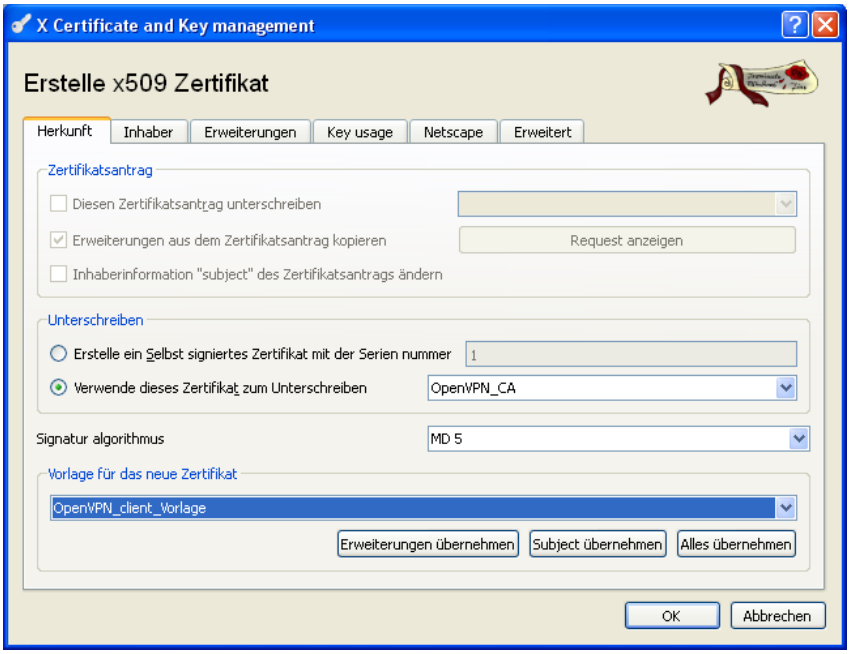
Gehen Sie auf **“Erstelle einen neuen Schlüssel”** und geben sie denselben Name ein wie der “**commonName**” des Zertifikates.



ERSTELLEN EINES CLIENT-ZERTIFIKATES

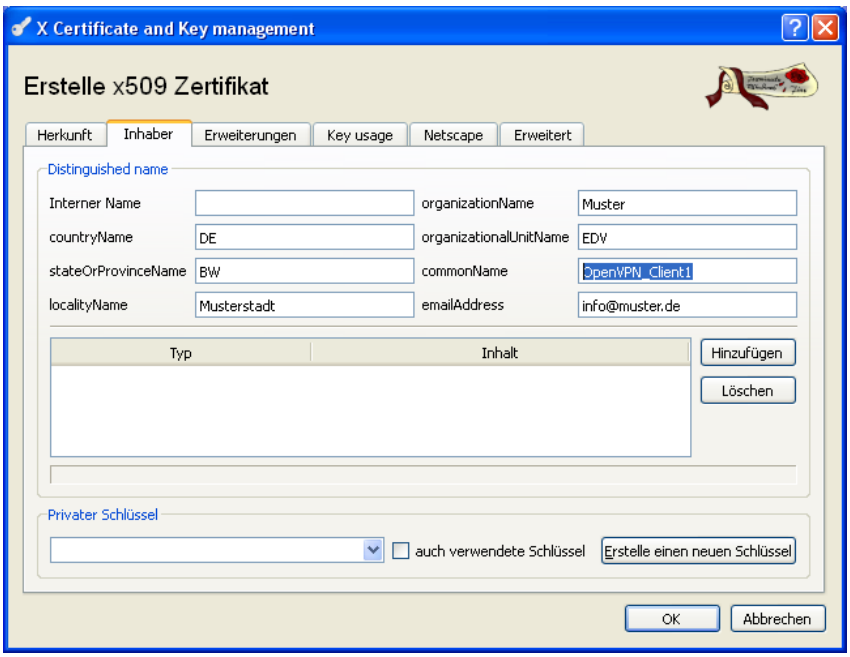
Für jeden Client muss ein eigenes Zertifikat erstellt werden.

Wiederholen sie alle Schritte wie bei dem Server-Zertifikat, wählen Sie nur diesmal die zuvor erstellte „**Client-Vorlage**“ aus.

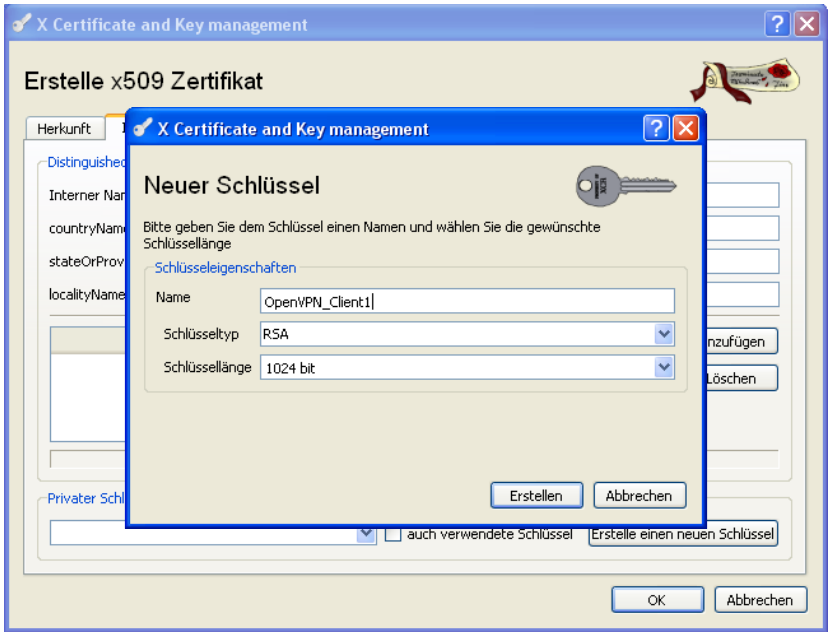


Hinweis:

- *jeder “commonName” muss eindeutig sein!*
- *Zum Beispiel: OpenVPN_Client1, OpenVPN_Client2, etc..*

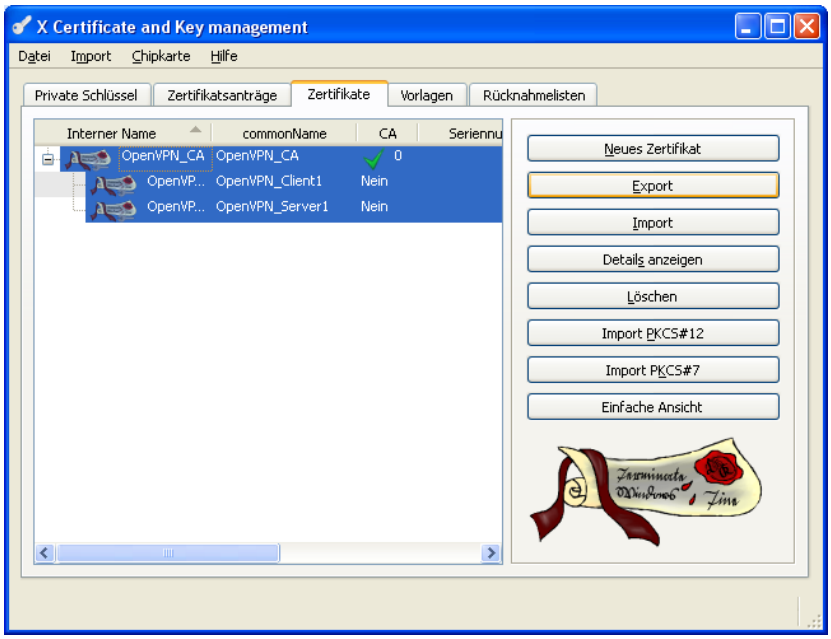


Für jeden Client muss nun jeweils ein neuer Schlüssel erstellt werden. (Name = commonName).



EXPORTIEREN ALS PKCS#12-DATEIEN

Zur Verwendung der Schlüsselpaare mit OpenVPN, können diese kompakt in eine PKCS#12-Datei exportiert werden. Hierzu wird unter dem Reiter "**Zertifikate**" die Schaltfläche "**Export**" verwendet.

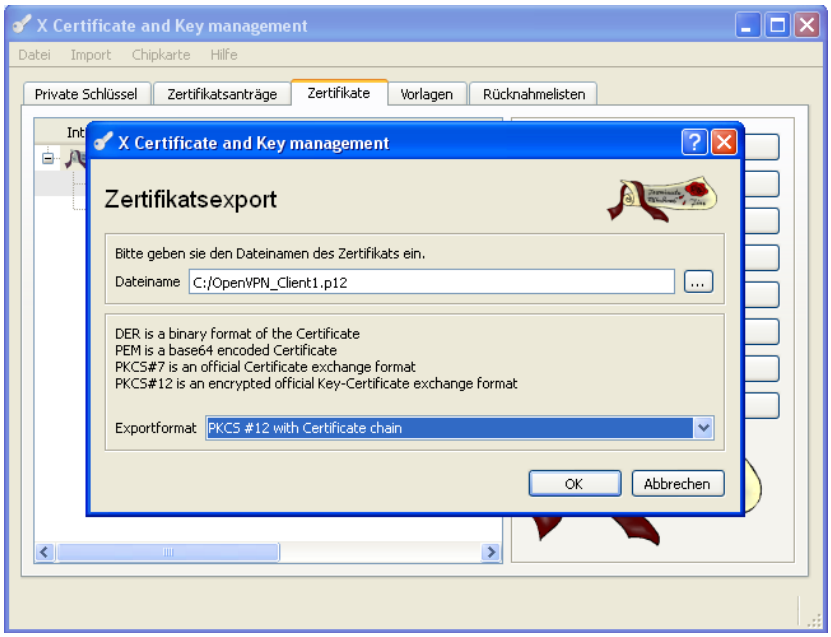


Markieren Sie nun alle Clients und Server, die exportiert werden sollen und klicken Sie auf die Schaltfläche „**Export**".

Wählen Sie nun das gewünschte Verzeichnis aus um die Clients und Server auf ihrem System abzulegen.

Hinweis:

- *Wählen Sie als Exportformat ausschließlich **"PKCS #12 with Certificate Chain**" um zu gewährleisten, dass das Zertifikat mit OpenVPN und dem Gerät richtig funktioniert.*



Zusätzlich können Sie die PKCS#12-Datei mit einem Passwort schützen. Beim Server sollten Sie jedoch kein Passwort verwenden, da dieses den Autostart auf Linux- und Windows XP -Systemen verhindern würde. Für das Gerät werden alle Passwörter nur einmal, während dem Hochladen der Zertifikate auf das Gerät, benötigt.

Bei der Verwendung der VPN-Clients unter Linux oder Windows muss das Passwort bei jeder neuen Verbindung mit dem Netzwerk eingegeben werden.

Unter Umständen kann es auch sinnvoll sein alle Felder leer zu lassen und kein Passwort zu vergeben. Anstatt eines Passworts kann auch eine Limitierung der zeitlichen Gültigkeit vor unerwünschter Nutzung schützen.

Tipp: Um die Server-Belastung zu verringern, können Sie auf dem Gerät einstellen, dass die VPN Verbindung erst über den Schlüsselschalter im Schaltschrank initialisiert wird.

Wenn Sie ein Passwort verwenden möchten, wählen Sie ein möglichst sicheres:

EINBINDEN DER ZERTIFIKATE IN OPENVPN

Wenn Sie die Zertifikate auf dem PC verwenden möchten, auf dem auch XCA läuft, müssen Sie nun - nach der Erstellung und dem Export der Zertifikate - diese noch in das OVPN Verzeichnis kopieren.

Wenn Sie die Zertifikate auf dem Gerät verwenden möchten, müssen Sie sicherstellen, dass das Gerät mit einem PC verbunden ist und Sie Zugriff auf das Web Interface haben.

Gehen Sie nun zu „**Allgemein / Zertifikate**“ und wählen Sie die “**Upload**” Schaltfläche. Suchen Sie nun nach dem Verzeichnis, in dem Ihre Zertifikate abgelegt wurden und wählen Sie mit einem Doppelklick dasjenige aus, welches Sie auf das Gerät hochladen möchten. Sollte das Zertifikat durch ein Passwort geschützt sein, müssen Sie nun das Passwort angeben.

Gehen Sie zu „**Konfiguration / OpenVPN**“ um Ihre OpenVPN Einstellungen zu konfigurieren. Das hochgeladene Zertifikat sollte nun in dem Drop-down Menü verfügbar sein.

Um die p12 Datei in einer normalen OpenVPN Konfiguration verwenden zu können geben nach dem folgenden Abschnitt:

SSL/TLS parms.

See the server config file for more

description. It's best to use

a separate .crt/.key file pair

for each client. A single ca

file can be used for all clients.

das Folgende ein:

pkcs12 "…OpenVPN\\cert\\OpenVPN_Client1.p12"

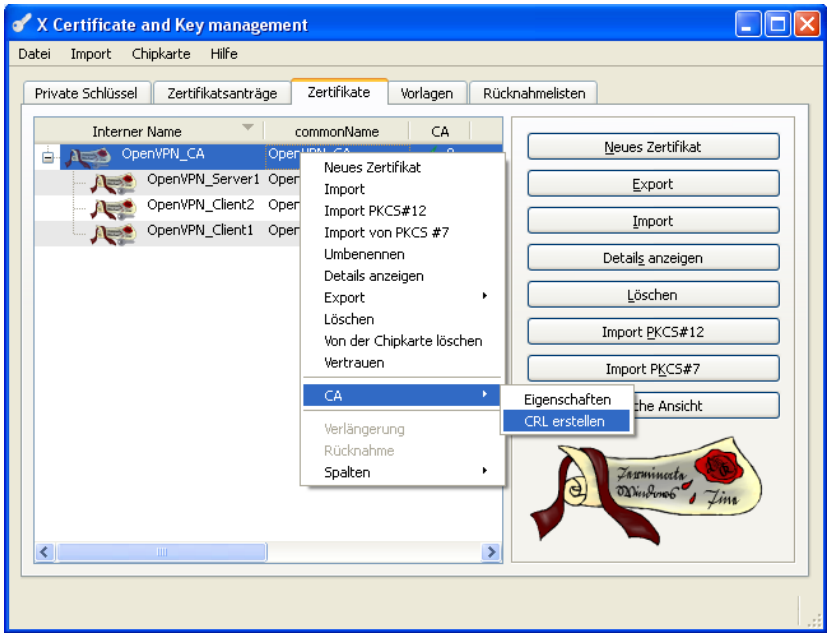
Alle anderen Dateitypen, die in der OVPN Datei beschrieben sind, können ignoriert werden.

ERSTELLEN EINER CRL (CERTIFICATE REVOCATION LIST)

XCA bietet zusätzlich eine Funktion zum Erstellen einer CRL auf der Grundlage ihrer CA und der Zertifikats-Kette (certificate chain).

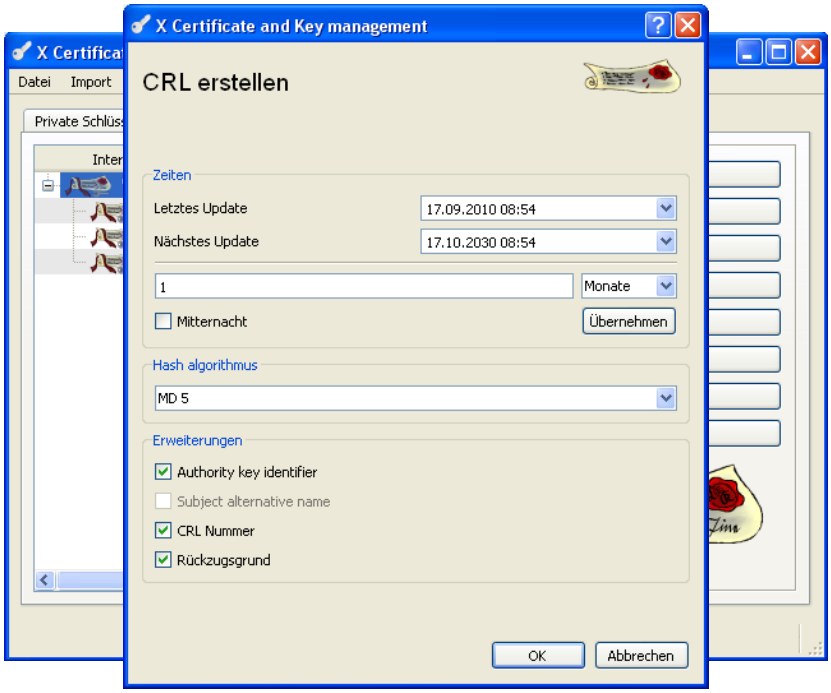
Bei einer CRL handelt es sich um eine Auflistung aller Zertifikate mit deren jeweiligem Gültigkeitsstatus. Hiermit können auf einfache Weise zentral am Server einzelne Zertifikate zurückgezogen werden.

Es handelt sich um eine spezielle Datei, die in XCA erstellt, und wie ein Zertifikat auf das Gerät hochgeladen werden kann.

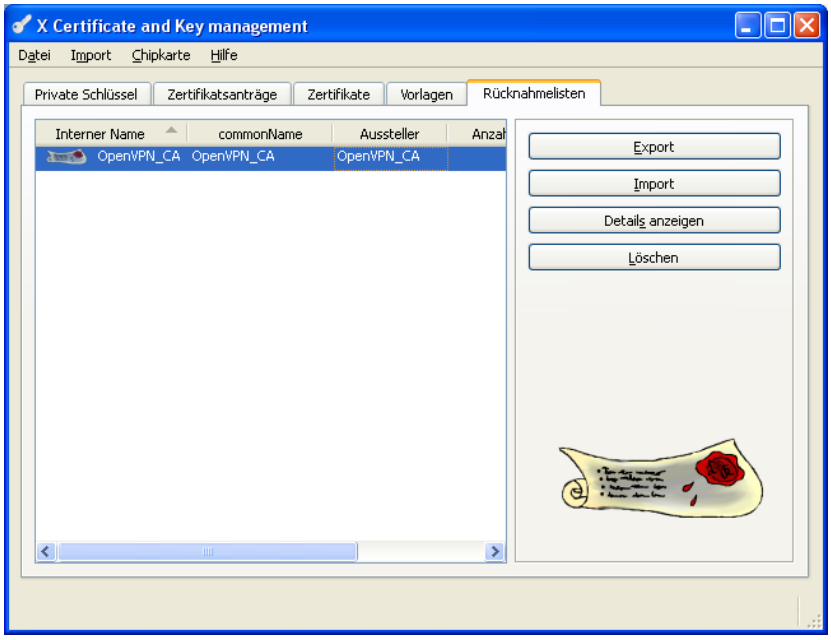


Sie müssen den Gültigkeitszeitraum bestimmen sowie den Zeitpunkt, an dem das nächste Update ausgeführt werden soll. Ihr nächstes Updatedatum sollte möglichst fern in der Zukunft liegen - in der Regel gibt es für die Erstellung eines neuen Zertifikates keinen anderen Grund, außer dem Verlust des alten Zertifikates.

Setzen Sie jeweils einen Haken in den drei Feldern, wie es auf dem nächsten Screenshot zu sehen ist, und klicken Sie dann auf „**OK**“.



Nach dem die CRL erstellt wurde, finden Sie diese unter dem letzten Reiter des Hauptmenüs: „**Rücknahmelisten**“.



Um die CRL auf das Gerät hochzuladen klicken Sie auf “**Export**”:

Wählen Sie „PEM“ als Dateiformat. Der von XCA vergebene Dateiname sollte durch die vorherige Auswahl bereits mit der richtigen Dateiendung versehen sein.

Die CRL PEM-Datei finden sie nun in dem Verzeichnis, in das bereits die anderen Zertifikate exportiert wurden. Um diese nun auf das Master Gerät hoch zu laden, müssen Sie genauso vorgehen wie beim Hochladen eines normalen Zertifikates:

Gehen Sie zum Web Interface **„Konfiguration / Allgemeine Einstellungen / Zertifikate**“, klicken Sie auf „Durchsuchen“ und wählen Sie die CRL aus. Anschließend laden Sie die Datei auf das Gerät über „**Zertifikat hochladen**“.

Alle installierten und eingebundenen Zertifikate werden gegen die neue CRL geprüft. Wenn Sie einem, zuvor widerrufenen Zertifikat wieder vertrauern möchten, müssen Sie dieses spezifische Zertifikat im XCA mit einem Rechtsklick anwählen und dessen Status auf „**Wieder vertrauen**“ ändern. Nachfolgend erstellen Sie eine neue CRL durch Exportieren und Hochladen wie oben beschrieben.

Wenn sie die Kopie des Zertifikates auf dem Gerät haben, werden sie feststellen, dass sich der Status auch im Web Interface auf „**Wieder vertrauen**“ geändert hat.

Dies kann nützlich sein um bestimmten Benutzern und Maschinen zeitweilig den VPN Zugang zu verwehren.

Hinweis:

- *Auch wenn die Gültigkeitsdauer einer Sperrliste abgelaufen ist, wird sie dennoch zur Überprüfung der Zertifikate verwendet solange keine aktuellere CRL vorhanden ist.*
- *Die Sperrlisten auf dem Gerät (maximal eine pro CA) sollten möglichst aktuell gehalten werden, damit keine Sicherheitslücken durch verlorengegangene Zertifikate entstehen.*

ERHÖHTE SICHERHEIT MIT DH:

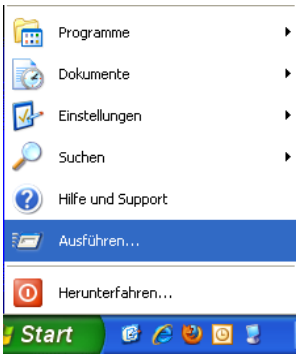
Aus Sicherheitsgründen empfiehlt es sich XCA mit einer eigenen DH-Datei zu verwenden.

Dies lässt sich mit OpenSSL umsetzen.

Falls Sie es nicht bereits haben, können Sie OpenSSL mit Standardoptionen unter dem folgenden Link herunterladen:

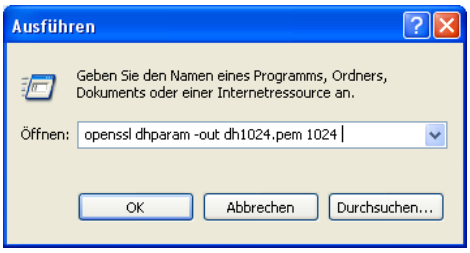
http://www.openssl.org/related/binaries.html

Nach der Installation wählen Sie im Startmenü “**Start & Ausführen**”. Hier tragen Sie “**CMD**” ein und drücken dann die Eingabetaste.



Wechseln Sie nun in das Verzeichnis: **C:\OpenSSL-Win32\bin** und geben den folgenden Befehl ein:

openssl dhparam -out dh1024.pem 1024



Die neue Datei dh1024.pem muss auf dem OpenVPN Server abgelegt werden und sorgt bei Verwendung zu erhöhter Sicherheit.

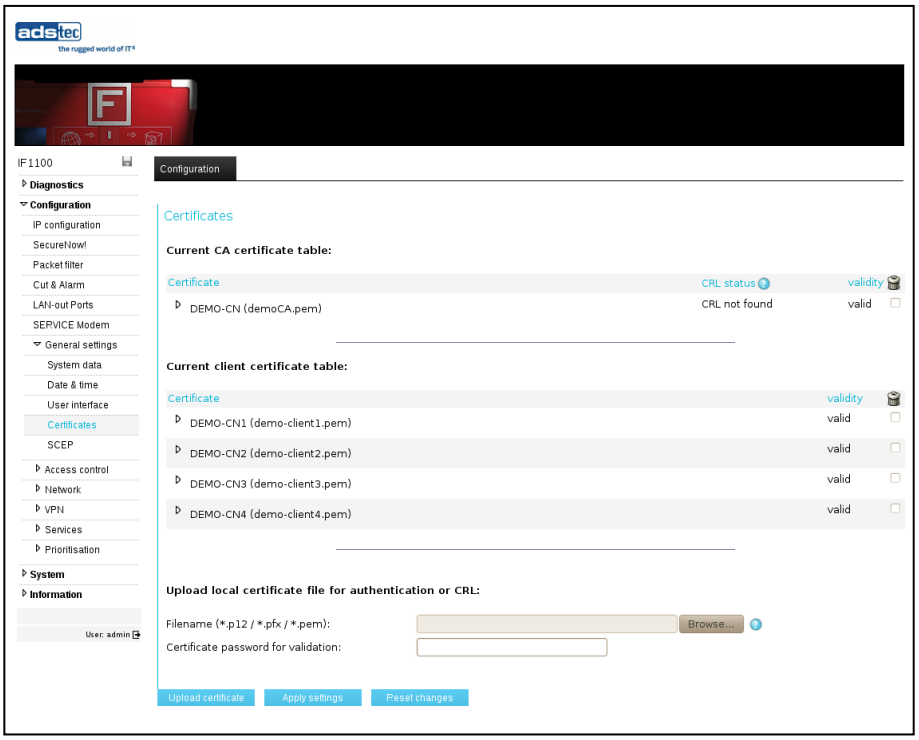
Zukünftig soll auch das Erstellen von DH-Dateien direkt in XCA integriert sein, in der verwendeten Version funktionierte dies aber nicht fehlerfrei.

ZUSÄTZLICHE HINWEISE

XCA bietet viele Möglichkeiten und weitere Funktionen, die zukünftig für Sie nützlich sein könnten. Bitte kontaktieren Sie uns falls Sie noch weitere Fragen haben oder zusätzliche Hilfe beim Erstellen ihrer Zertifikate benötigen.

HOCHLADEN VON ZERTIFIKATEN AUF DAS GERÄT

Sowohl CA-Zertifikate, normale Zertifikate (Client-Zertifikate) als auch Sperrlisten werden einheitlich über das Interface für Zertifikate auf das Gerät hochgeladen. Wird ein gültiges CA-Zertifikat auf dem Gerät gespeichert, so gelten für das Gerät alle Zertifikate, die von dieser CA signiert wurden, als vertrauenswürdig, sofern sie nicht in einer CRL aufgeführt sind.



Sollte der PKCS12-Container oder das Zertifikat selbst mit einem Passwort versehen sein, muss dieses beim Upload mit angegeben werden. Der Upload selbst erfolgt dann mittels „Upload certificate“.

Hinweis:

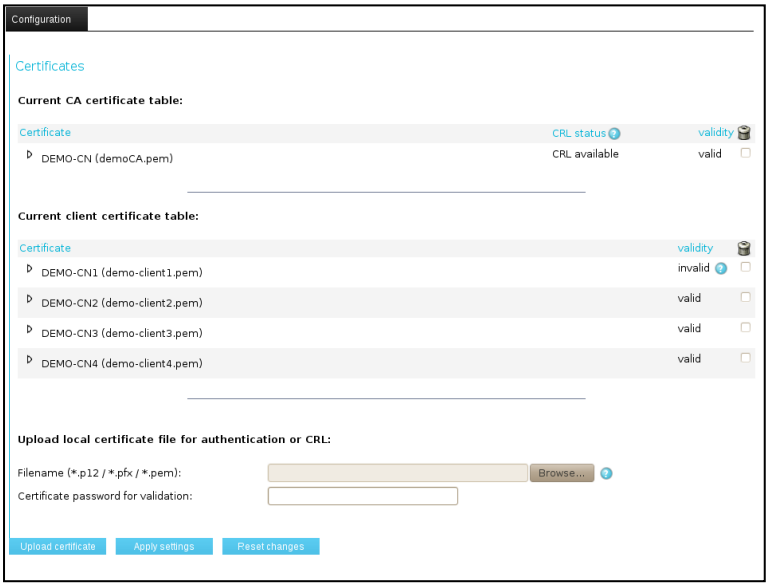
Für den Upload auf das Gerät muss ein Zertifikat entweder als PKCS12-Datei oder im PEM-Format mit integriertem privaten Schlüssel vorliegen.

Der private Schlüssel (z.B. myClient1.key) muss vor fremden Zugriff geschützt werden.

Im Fall einer externen CA wird die Zertifikatsanfrage generiert und der Zertifizierungsstelle zugesandt. Diese prüft die angegebenen Informationen und (falls diese in Ordnung sind) signiert die Anfrage. Das so entstandene Zertifikat kann dann zur Authentifizierung verwendet werden.

Um ein Zertifikat zu löschen, muss das Häkchen neben dem gewünschten Zertifikat unterhalb des Mülltonnensymbols gesetzt und „Apply Settings“ geklickt werden.

Sollte für ein CA-Zertifikat eine Sperrliste vorliegen, wird dies in der Spalte „CRL status“ angezeigt.



Hinweis:

Für den Upload eines Zertifikats als PEM-Datei muss der private Schlüssel im Zertifikat enthalten sein. Dies gilt nicht für CA-Zertifikate.

Eine CRL kann nur erfolgreich hochgeladen werden, falls das zugehörige CA-Zertifikat bereits auf dem Gerät existiert.

Wird ein CA-Zertifikat gelöscht, wird automatisch die zugehörige CRL-Datei gelöscht.

Die CA-Zertifikate demoCA.pem beziehungsweise myCA.pem sowie die damit signierten Zertifikate demo-clientX.pem beziehungsweise myClientX.pem dienen ausschließlich zu Testzwecken und dürfen nicht zur Authentifizierung verwendet werden!

FEHLERMELDUNGEN FÜR HOCHGELADENE ZERTIFIKATE

Ob ein erfolgreich hochgeladenes Zertifikat auch wirklich verwendet werden kann, wird in der Spalte Gültigkeit angezeigt. Sollte es nicht verwendet werden können, kann man auf das kleine Fragezeichen klicken, um die genaue Fehlermeldung zu sehen.

Falls das Zertifikat noch nicht oder nicht mehr gültig ist, erscheint die Meldung:

error 9 at 0 depth lookup: certificate is not yet valid

Lösung: Die Systemzeit muss korrekt eingestellt werden. Oder falls es sich um ein tatsächlich ungültiges Zertifikat handelt, muss vom Herausgeber ein neues Zertifikat angefordert werden.

Falls zu einem normalen Zertifikat das passende CA-Zertifikat fehlt, erscheint die Meldung:

error 20 at 0 depth lookup: unable to get local issuer certificate

Lösung: Das entsprechende CA-Zertifikat muss hochgeladen werden.

Falls ein normales Zertifikat hochgeladen wird und fälschlicherweise die exakt gleichen Identitätsangaben wie das CA-Zertifikat verwendet, mit dem es signiert wurde, dann erscheint die Meldung:

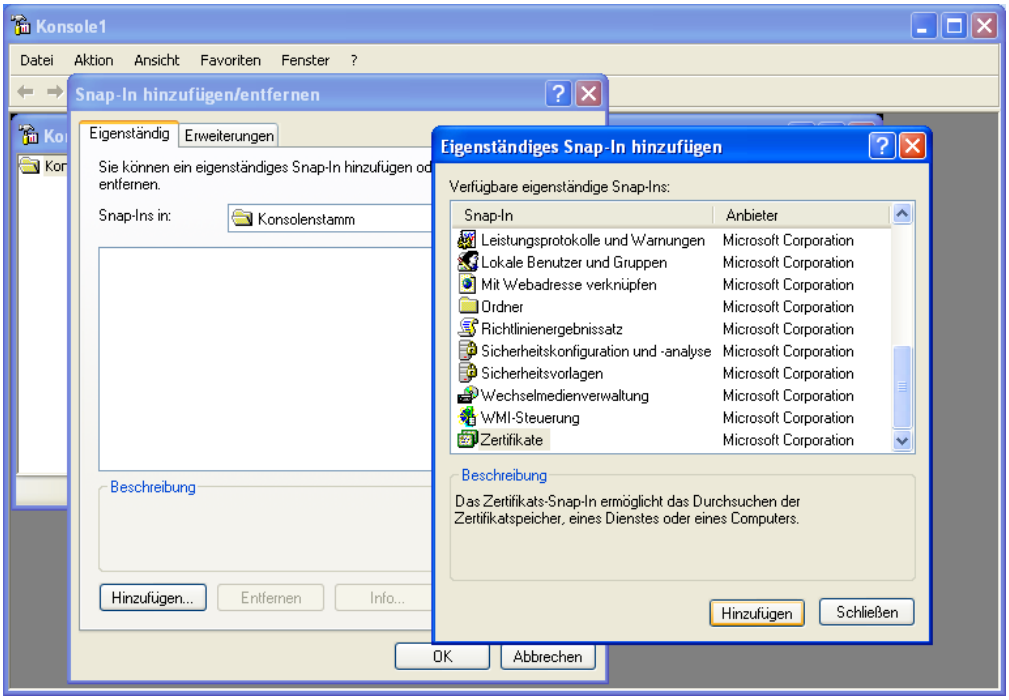
error 7 at 0 depth lookup: certificate signature failure

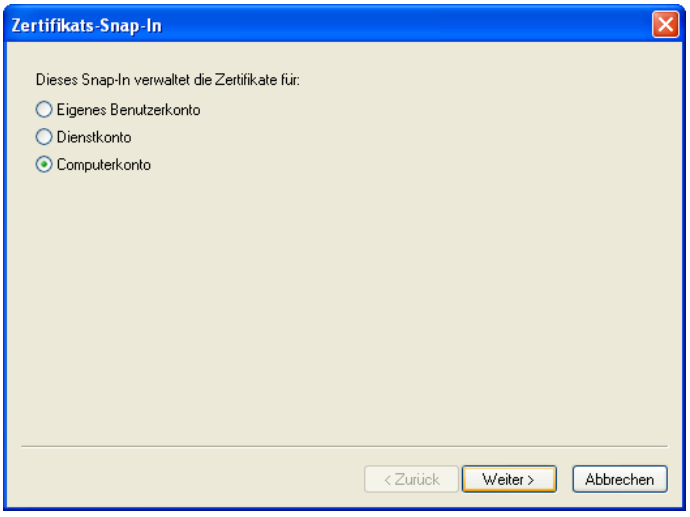
Lösung: Das Zertifikat muss neu gemacht werden. Dazu muss zunächst ein neues Client-Request erstellt werden und mindestens ein Identitätsfeld (zum Beispiel der Common Name) von den Einträgen des CA-Zertifikats unterschiedlich sein.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

IMPORTIEREN VON ZERTIFIKATEN UNTER WINDOWS

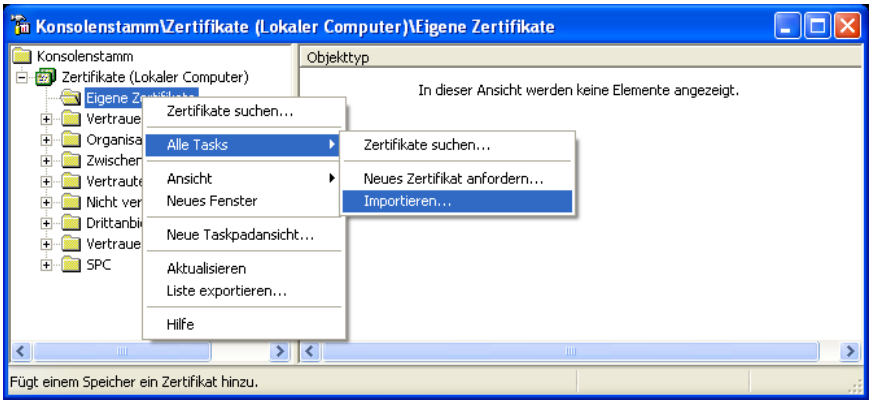
Zunächst muss die „Microsoft Management Console“ gestartet werden. Dazu in Start/Ausführen… den Befehl mmc eingeben. In der Konsole muss über Datei/Snap-In hinzufügen/entfernen… das Snap-In Zertifikate für das Computerkonto des lokalen Rechners geladen werden:



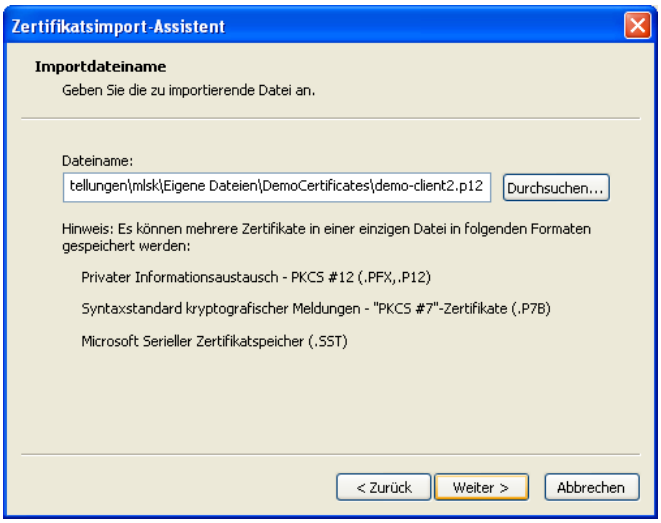


Computer auswählen
Wählen Sie den Computer aus, den dieses Snap-In verwalten soll.
Dieses Snap-In verwaltet:
Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)
Anderen Computer:
Durchsuchen...
Änderungen zulassen, wenn die Konsole von der Befehlszeile aus gestartet wird. Dies gilt nur, wenn die Konsole zuvor gespeichert wurde.
< Zurück
Fertig stellen
Abbrechen

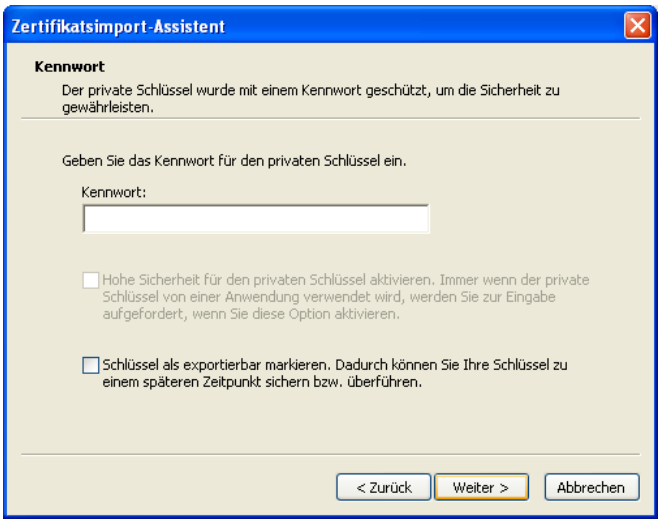
Mit einem Rechtsklick auf den Zertifikatsordner wird das Menü geöffnet. Über All Tasks/Importieren… wird dann der Zertifikatsimport-Assistent gestartet:



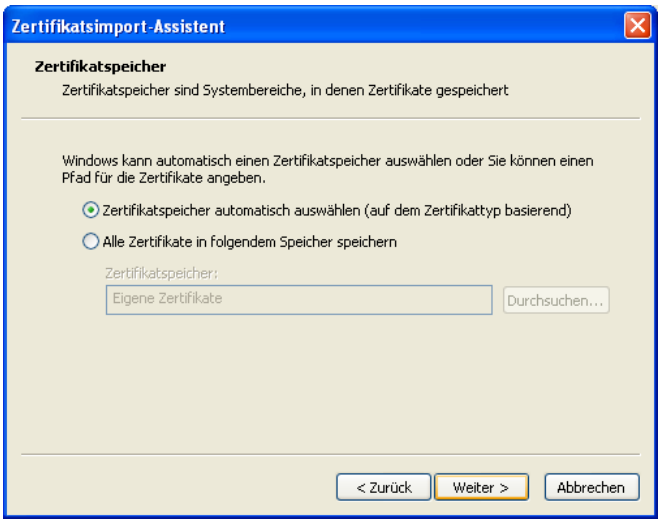
Als nächstes muss die Zertifikatsdatei ausgewählt werden:


Zertifikatsimport-Assistent
Importdateiname
Geben Sie die zu importierende Datei an.
Dateiname:
tellungen\mlsk\Eigene Dateien\DemoCertificates\demo-client2.p12
Durchsuchen...
Hinweis: Es können mehrere Zertifikate in einer einzigen Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Microsoft Serieller Zertifikatspeicher (.SST)
< Zurück
Weiter >
Abbrechen

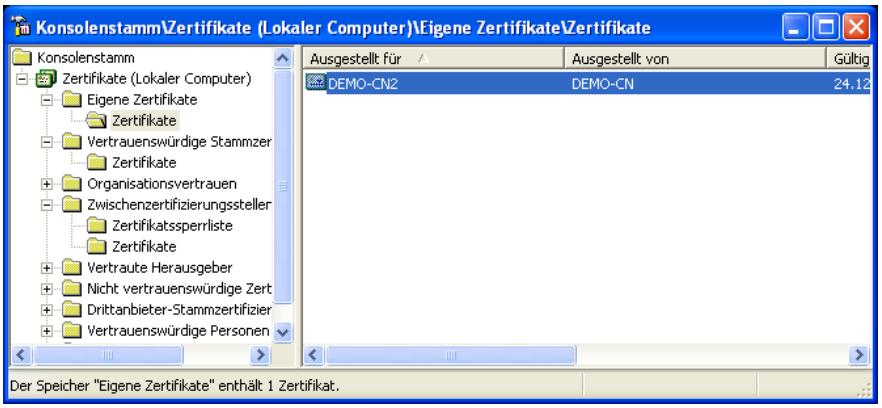
Sollte der Container oder das Zertifikat mit einem Passwort geschützt sein, muss dieses für den Import angegeben werden (für den Beispielcontainer demo-client2.p12 existiert kein Passwort, deswegen kann direkt Weiter geklickt werden):

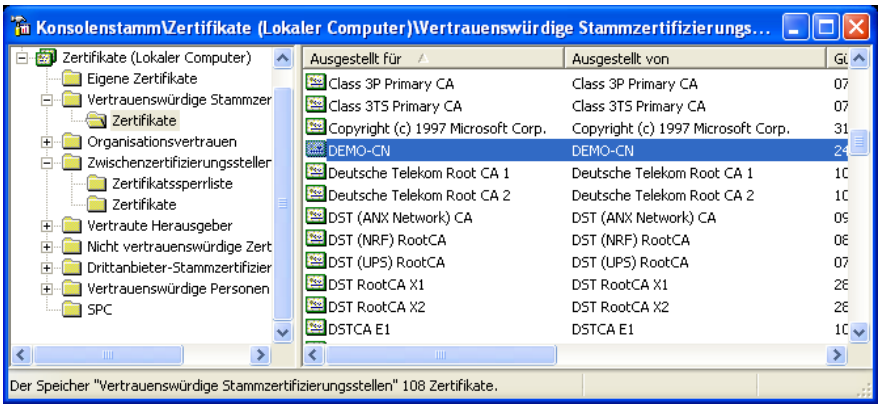

Zertifikatsimport-Assistent
Kennwort
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.
Geben Sie das Kennwort für den privaten Schlüssel ein.
Kennwort:
Hohe Sicherheit für den privaten Schlüssel aktivieren. Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie zur Eingabe aufgefordert, wenn Sie diese Option aktivieren.
Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
< Zurück
Weiter >
Abbrechen

Die Einordnung der Zertifikate muss automatisch erfolgen (damit zum Beispiel aus dem PKCS12-Container demo-client2.p12 demo-client2.pem als Zertifikat und demoCA.pem als Stammzertifikat einsortiert wird):


Zertifikatsimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Eigene Zertifikate
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Abschließend muss der Import fertiggestellt werden. Die Zertifikate können dann unter Eigene Zertifikate und die Stammzertifikate unter Vertrauenswürdige Stammzertifikate eingesehen werden. Eventuell müssen diese Verzeichnisse erst aktualisiert werden (Rechtsklick und im Menü den Punkt Aktualisieren auswählen).





Hinweis:

- *Die PKCS12-Datei demo-client2.p12 enthält neben dem eigentlichen Zertifikat demo-client2.pem auch das Stammzertifikat demoCA.pem.*
- *Sollte bei eigenen Zertifikaten das Stammzertifikat nicht im Container enthalten sein, muss dieses analog importiert werden.*

12.3 SIM-KARTE

ALLGEMEIN

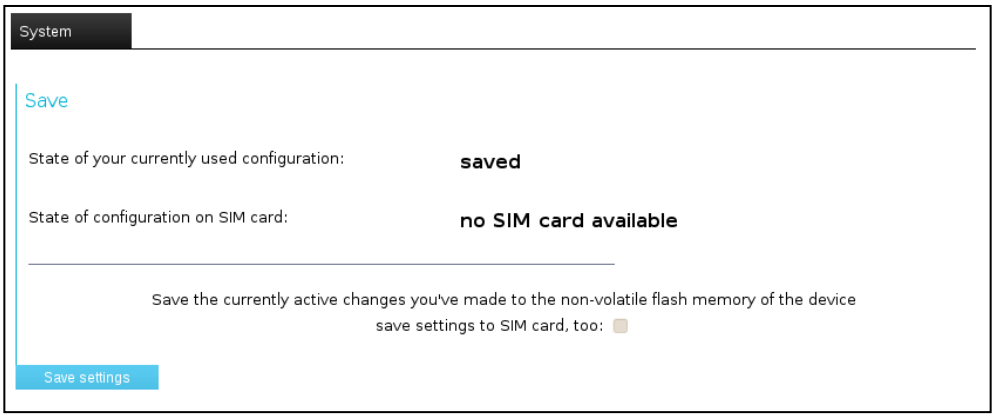
Mit Hilfe der SIM-Karte kann ein defektes Gerät einfach ausgetauscht werden. Es muss lediglich die SIM-Karte aus dem defekten Gerät in das Ersatzgerät eingelegt werden. Ein Eingreifen von qualifiziertem Personal ist nicht nötig.

ART DER SIM KARTE

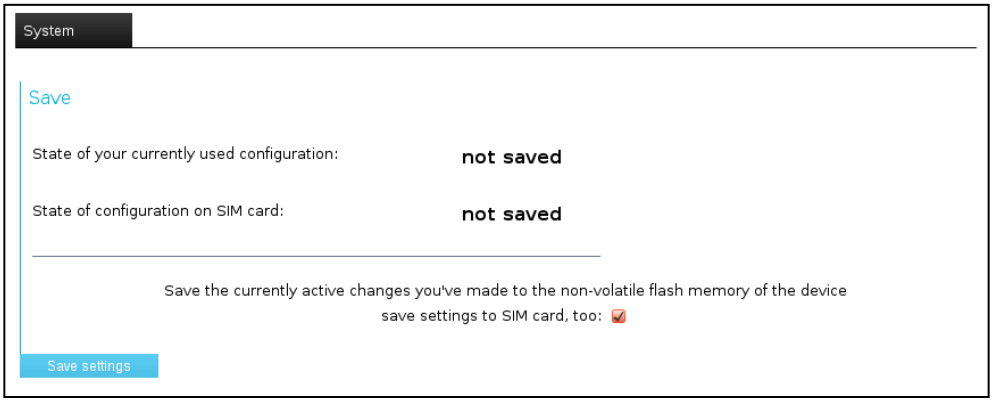
Es können nur SIM-Karten von ads-tec verwendet werden!

SPEICHERN DER KONFIGURATION AUF DER SIM-KARTE

Ist keine SIM-Karte eingelegt erscheint die Meldung „keine SIM-Karte verfügbar“.


System
Save
State of your currently used configuration:
saved
State of configuration on SIM card:
no SIM card available
Save the currently active changes you've made to the non-volatile flash memory of the device
save settings to SIM card, too:
Save settings

Um die Einstellungen auf der SIM-Karte zu speichern muss im „Speichern“ Dialog die Checkbox „Einstellungen ebenfalls auf SIM-Karte schreiben“ aktiviert werden und anschließend der Speichern Button betätigt werden.


System
Save
State of your currently used configuration:
not saved
State of configuration on SIM card:
not saved
Save the currently active changes you've made to the non-volatile flash memory of the device
save settings to SIM card, too:
Save settings

ERSETZEN EINES GERÄTES

SIM-Karte in ausgeschaltetes Gerät einlegen und dann das Gerät anschalten. Die Einstellungen werden nun beim Booten geladen. Im Eventlog können folgende Meldungen erscheinen:

BEISPIELE:

erfolgreiches zurücklesen der Einstellungen:

Nov 1 00:00:05 IF1xxx system: successfully loaded config from SIM card

erfolgreiches Update der SIM Karte auf andere Firmware als vorher gespeichert:

Nov 1 00:00:05 IF1xxx system: successfully updated SIM card config to firmware version: 1.1.1

Hinweis:

Wird eine SIM-Karte auf einem Gerät mit einer aktuellen Firmware gespeichert und anschließend in ein Gerät mit älterer Firmware eingelegt so werden automatisch alle neuen vorgenommenen neuen Parameter der neueren Firmware gelöscht da diese nicht auf der alten Firmware verfügbar sind. Dies gilt auch für die Daten auf der SIM-Karte selbst.

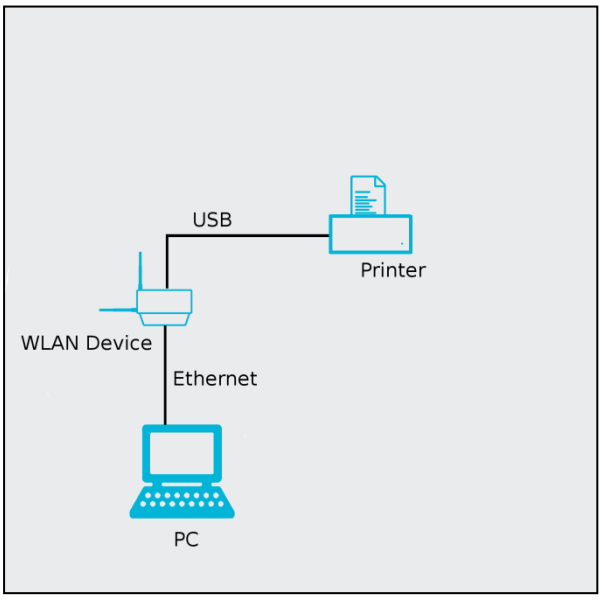
(Gilt nur für RAP/RAC!) Eine SIM-Karte mit Konfiguration kann nicht zwischen zwei verschiedenen Geräte-Typen ausgetauscht werden. Wird z.B. die Konfiguration auf einem RAP111x auf die SIM Karte gespeichert so wird die SIM-Karte nicht lesbar sein wenn man sie in einen RAC111x einlegt. Ein Überschreiben der Karte ist jedoch jederzeit möglich.

RAP/RAC Geräte mit einer älteren Hardwarerevision beherrschen trotz vorhandenem SIM-Kartenslot die Funktion nicht. In diesen Fällen sind die SIM-Karten Funktionen nicht sichtbar.

12.4 USB-DRUCKER

ALLGEMEIN

WLAN Geräte, die über USB Ports verfügen können genau ein USB Drucker für das Netzwerk freigeben. Es ist keine Konfiguration auf Seiten der WLAN Geräte notwendig. Weiterhin wird immer der erste erkannte Drucker auf dem TCP Port 9100 bereitgestellt. Die Anbindung des Druckers kann wie abgebildet über Ethernet oder aber auch über WLAN erfolgen.



KONFIGURATION

Konfiguration des Druckers unter Windows XP

- Der Hersteller Druckertreiber muss installiert werden, falls Windows den zu verwendenden Drucker nicht von Haus aus unterstützt.
- In der Systemsteuerung können unter „**Drucker und Faxgeräte**“ neue Drucker hinzugefügt werden. Hierzu den Menüpunkt „**Drucker hinzufügen**“ über das Dateimenü auswählen.
- In dem darauffolgenden Dialog „**Lokaler Drucker**“ auswählen und mit „**Weiter**“ bestätigen.
- In dem Dialogfenster „**Druckeranschluss**“ muss „**Einen neuen Anschluss erstellen**“ ausgewählt werden und im Menü der Eintrag „**Standard TCP/IP Port**“. Auf „**Weiter**“ klicken.
- Das Feld Drucker oder IP-Adresse ausfüllen und „**Weiter**“ klicken.
- Im nächsten Schritt muss „**Benutzerdefiniert**“ ausgewählt werden und über „**Einstellungen**“ der Port 9100 eingegeben sowie als Protokoll RAW ausgewählt werden.
- Nach Beendigung des Druckeranschluss-Wizards muss der richtige Drucker Treiber ausgewählt werden, danach ist die Installation beendet.

KONFIGURATION DES DRUCKERS UNTER LINUX MIT HILFE VON CUPS

- Die CUPS Konfiguration wird mit Hilfe eines Browsers unter der Adresse **http://localhost:631** gestartet.
- Über den Eintrag „**Drucker hinzufügen**“ wird der Wizard gestartet.
- Auf der ersten Seite muss mindest der Drucker Name ausgefüllt werden, alle anderen Informationen sind optional.
- Im nächsten Schritt muss „**Internet Printing Protocol (IPP)**“ ausgewählt und mit „**Fortsetzen**“ bestätigt werden.
- In dem Feld URI muss die IP-Adresse und der Port in der Form**: socket://<IP>:<PORT>** eingetragen werden. Wobei der Port fest auf 9100 gesetzt werden muss.
- Im letzten Schritt muss noch der richtige Druckertreiber ausgewählt werden, dann ist der Wizard abgeschlossen.

12.5 Übersicht der Client Betriebsmodi

Wireless Netzwerke werden immer komplexer und vielfältiger. Eine riesige Anzahl unterschiedlicher Hersteller und Funktionen macht die Anbindung weiterer Clients meist immer schwieriger. Dieser Use Case soll dabei helfen den passenden Betriebsmodus des ads-tec WLAN Clients zu ermitteln und so die bestmögliche Performance beim Roaming zu erreichen.

Access-Point	Bridgemodus (für nicht Router Betriebsmodi)	Roamingmodus Single Client	Roamingmodus Dual Client
nicht ads-tec kompatibel	MCB / SCB	Standard Roaming	Extended Background Scanning
ads-tec kompatibel	FTB	Standard Roaming	Extended Background Scanning
Wireless Controller ohne Sicherheitsmaßnahmen (z.B.: Motrolla)	MCB / SCB	Standard Roaming	Extended Background Scanning
Wireless Controller mit Sicherheitsmaßnahmen (z.B.: Cisco)	-	Standard Roaming im Router Modus	Extended Background Scanning & IP Router
ads-tec Access-Point	FTB	Standard Roaming	Seamless Roaming

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

BRIDGEMODUS

Die ads-tec WLAN Clients kennen 3 unterschiedliche Bridgemodi.

FTB (**F**ully **T**ransparent **B**ridge): Kann für ads-tec kompatible Access-Points verwendet werden. Dabei können alle Geräte hinter dem WLAN Client auf Layer 2 angesprochen werden.

Für alle nicht kompatible ads-tec Access-Points wird einer der folgenden Bridgemodi benötigt.

MCB (**M**ulti **C**lient **B**ridge): Aller Ethernetteilnehmer hinter dem WLAN Client werden mit der MAC-Adresse der WLAN Schnittstelle maskiert. Dabei wird das erste Gerät voll auf Layer 2 transparent maskiert, die restlichen Geräte erhalten Layer 3 transparenten Zugriff (d.h. nur noch Protokoll Daten können übertragen werden).

SCB (**S**ingle **C**lient **B**ridge): Hier wird genau ein Ethernetteilnehmer maskiert, dieser erhält vollen Layer 2 transparenten Zugriff, muss aber manuell mit seiner MAC-Adresse im Webinterface des WLAN Clients eingestellt werden.

Hinweis:

Im Betriebsmodus IP Router oder Extended Background Scanning & IP Router wird kein Bridgemods benötigt, die Konfigurationsseite ist deaktiviert.

ROAMINGMODI

- Standard Roaming: Es stellt das langsamste aller Roamingmodi dar. Hierbei werden Kriterien definiert, nach denen der WLAN Client zurück in den Scan-Zustand fällt und alle Kanäle absucht. Je nach Anzahl der zu scannenden Kanäle kann dies mehrere Sekunden Zeit beanspruchen.
- Extended Background Scanning: In diesem Roamingmodi hält eine WLAN Schnittstelle die Datenverbindung aufrecht, während die Zweite nach weiteren Access-Points sucht. Werden die konfigurierbaren Kriterien für einen Access-Point Wechsel unterschritten, dann bucht sich die ersten WLAN Schnittstelle direkt beim neuen Access-Point ein. Das Scannen entfällt und somit sind Romaingzeiten von 10 – 50ms möglich.
- Extended Background Scanning & IP Router: Dieser Roamingmodus unterscheidet sich in den Roamingeigenschaften nicht vom Extended Background Scanning. Jedoch ist dieser Modus durch die Kombination mit dem IP Routermodus in der Lage ein weiteres IP-Netz hinter seiner WLAN Schnittstelle aufzubauen. In Zusammenarbeit mit NAT und Portforwarding können so maskierte Zugriffe trotz Sicherheitsfunktionen auf Wireless Controllern realisiert werden.
- Seamless Roaming: Dieser Roamingmodus funktioniert nur in Kombinantion mit ads-tec Access-Points. Beide Schnittstellen bauen Datenverbindungen auf, wobei jeweils nur eine Schnittstelle aktiv Daten sendet. Bei Bedarf werden die Rollen gewechselt. So lassen sich unterbrechungsfreie Roamingvorgänge realisieren.

© ads-tec GmbH • Heinrich-Hertz-Str. 1 • 72622 Nürtingen

12.6 Extended Backround Scanning und Router

Mit dem zunehmenden Einsatz von Wireless Controllern sind auch weitere Sicherheitsfunktionen in die WLAN-Netzwerke eingebaut worden. So filtern zum Beispiel moderne Wireless Controller Ethernetpakete und blockieren WLAN Clients, sobald diese Clients mehr als eine IP-Adresse verwenden. Dies führt immer dann zu Problemen, wenn Ethernetsegmente gebrigded werden sollen, also hinter dem WLAN Client noch weitere, meist per Ethernet angebundene, Geräte betrieben werden sollen.

Um diesem Problem zu begegnen, ist es nötig sicherzustellen, dass auf Seiten des Wireless Controller nur eine IP-Adresse pro WLAN Client verwendet wird. Hierzu kann der WLAN Client gleichzeitig in 2 Netzwerken sein, eines für die Wireless Schnittstelle und ein weiteres für die Ethernet Schnittstelle. Allerdings werden dann Routingfunktionen auf dem WLAN Client und entsprechende Gateway Einträge auf allen beteiligten Geräten benötigt.

Um die Konfiguration zu Vereinfachen bietet es sich an, auf dem WLAN Client NAT (Network Address Translation) zu aktivieren. Damit müssen die Geräte im Wireless Netzwerk nicht mehr von dem privaten Ethernet Netzwerk hinter dem Client Kenntnis haben. Die Ethernet Teilnehmer werden also „verschleiert“.

Des Weiteren kann durch Portforwarding ein direktes ansprechen einzelner Ethernet Clients hinter einem NAT Router ermöglicht werden, so dass zum Beispiel ein Server innerhalb des Wireless Netzwerks die Geräte hinter dem WLAN Client abfragen kann. Andernfalls müsste jede Kommunikation immer von den Ethernet Clients ausgehen.

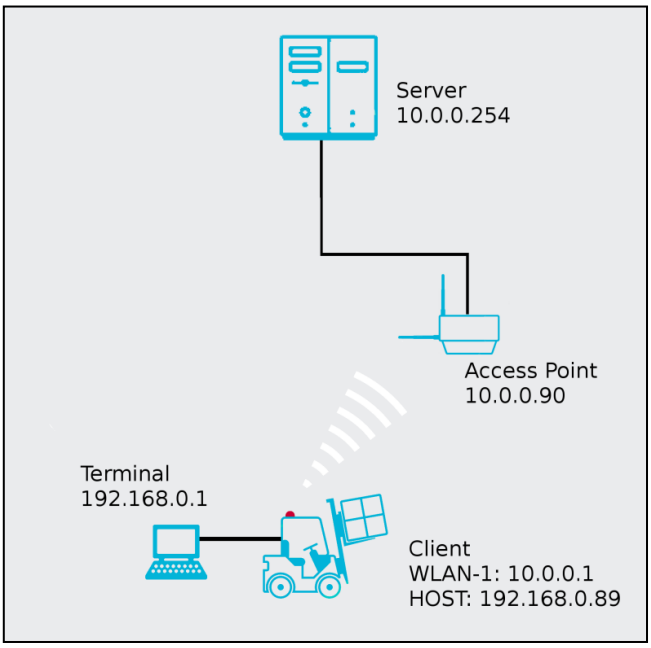
Die ads-tec WLAN Geräte bieten für solche Umgebungen den sogenannten „Extended Background Scanning und IP Router“ Modus an, dessen Konfiguration im folgenden erläutert wird.

<u>Beispielhaft wird die Konfiguration anhand folgender Topologie erklärt:</u>

→192.168.0.0/255.255.255.0 ist das private verschleierte Netzwerk hinter den WLAN Clients.

→10.0.0.0/255.255.255.0 ist das eigentlich WLAN Netzwerk, in dem sich die Access-Points und Clients (WLAN-1 Schnittselle) befinden.

→Auf dem Terminal muss die korrekte Gateway Adresse konfiguriert werden. Im Beispiel ist das die HOST Adresse des WLAN Clients (192.168.0.89)



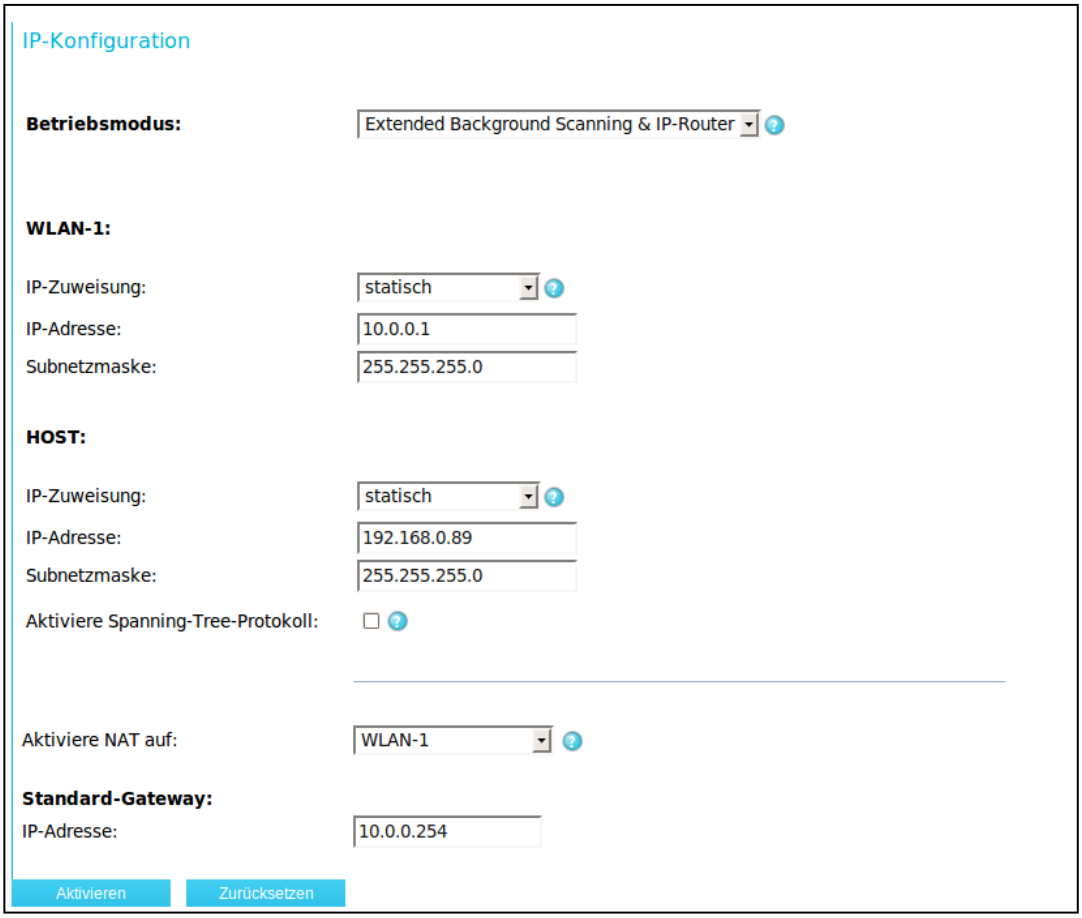
Hinweis:

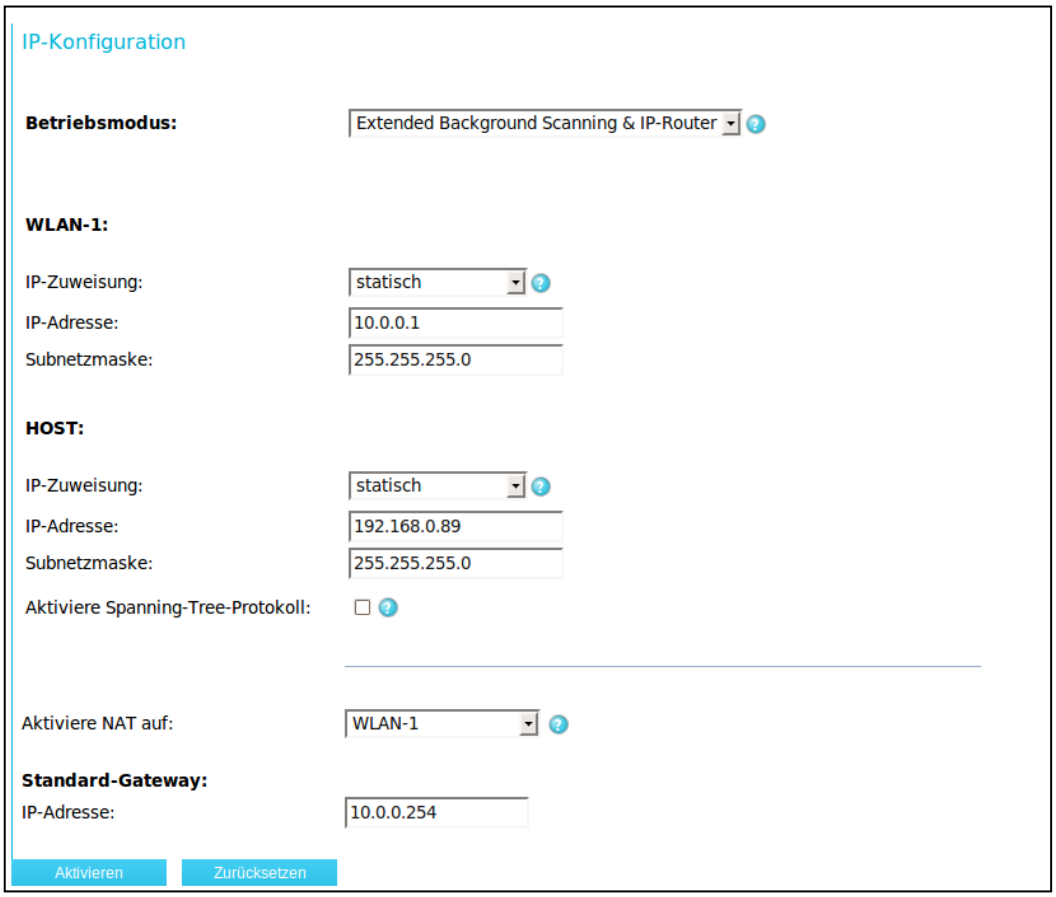
Das private Netzwerk kann beliebig oft in identischer Konfiguration innerhalb des gesamten Setups auftauchen. Es ist also möglich alle Terminals mit der IP 192.168.0.1 und alle WLAN Clients auf der HOST Schnittstelle mit der IP 192.168.0.89. Lediglich die WLAN-1 IP Adresse muss eindeutig im Netzwerk sein, hier kann aber auch mit einem DHCP Server gearbeitet werden.

AKTIVIEREN DES EXTENDED BACKGROUND SCANNING UND IP ROUTER MODUS

Um den WLAN CLient in den „Extended Background Scanning und IP Router“ Modus zu setzen muss man den Betriebsmodus unter „**Konfiguration → IP-Konfiguration**“ entsprechend ändern.

Dabei gilt es zu beachten, dass NAT auf der WLAN-1 Schnittstelle aktiviert wird, wenn eine „**Verschleierung**“ gewünscht wird. Andernfalls muss für korrekte Routen im gesamten Wireless Netzwerk gesorgt werden.


IP-Konfiguration
Betriebsmodus:
Extended Background Scanning & IP-Router
WLAN-1:
IP-Zuweisung:
statisch
IP-Adresse:
10.0.0.1
Subnetzmaske:
255.255.255.0
HOST:
IP-Zuweisung:
statisch
IP-Adresse:
192.168.0.89
Subnetzmaske:
255.255.255.0
Aktiviere Spanning-Tree-Protokoll:
Aktiviere NAT auf:
WLAN-1
Standard-Gateway:
IP-Adresse:
10.0.0.254
Aktivieren
Zurücksetzen



Hinweis:
Sobald das Gerät diesem Modus betrieben wird, sind die Konfigurationsseiten für die zweite WLAN-Schnittstelle inaktiv!

Hinweis:
Für beide WLAN-Schnittstellen wird das Nachbar-Roaming aktiviert, dies wird auch nach dem Deaktivieren des Operationsmodus beibehalten!

KONFIGURATION DER WLAN-SCHNITTSTELLE(N)

Die weitere Konfiguration der WLAN-Schnittstelle kann wie gewohnt unter

- **Konfiguration → WLAN-1 Parameter**
- **Konfiguration → WLAN-1 Sicherheit**
- **Konfiguration → Adv. WLAN → Roaming WLAN-1**

vorgenommen werden.

Dabei kann nur die WLAN-1 Schnittstelle konfiguriert werden, die Einstellungen werden automatisch auf die zweite Schnittstelle angewandt.

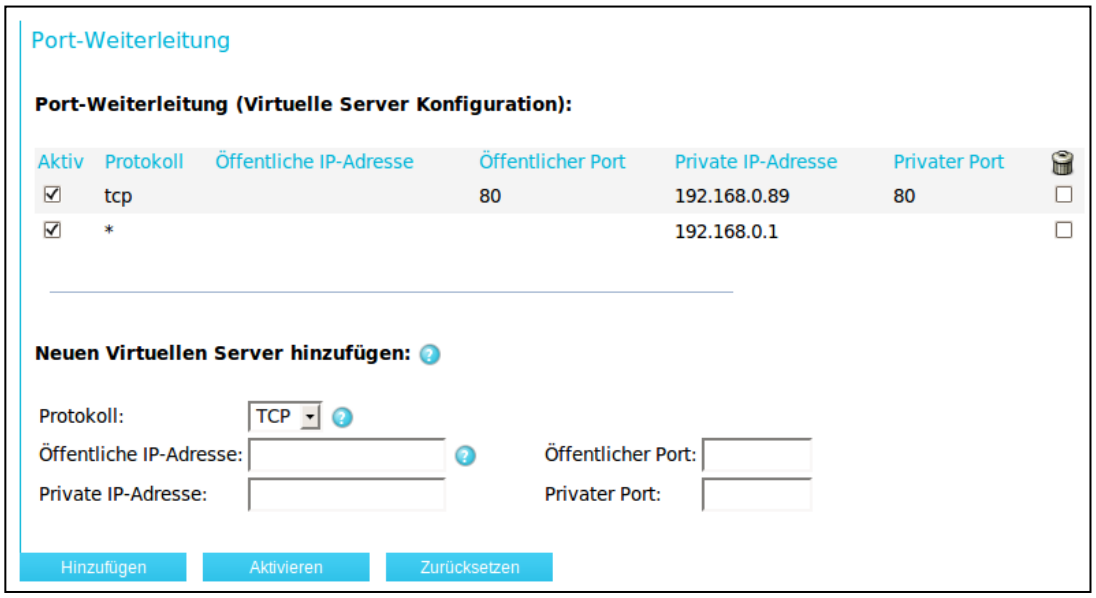
Hinweis:
Die Antenneneinstellungen können für beide WLAN-Schnittstellen auf den jeweiligen Seiten vorgenommen werden.

KONFIGURATION DES PORTFORWARDING

Unter Konfiguration → Netzwerk → Port-Weiterleitung können Regeln definiert werden, die die eingehenden Ethernetpakete weiterleiten. Somit ist es möglich das „**verschleirte**“ Terminal direkt aus dem WLAN Netzwerk (10.0.0.0) heraus abzusprechen, ohne dessen IP Adresse zu kennen.

Die erste Regel leitet alle http Anfragen (Port 80) zum WLAN Client selbst um, somit kann dessen Webinterface in gewohnter Art angesprochen werden.

Erst die zweite Regel leitet alle restlichen Pakete (TCP und UDP) aller übrigen Ports zum Terminal (192.168.0.1) weiter.



Hinweis:

Mit diesen Einstellungen ist es nicht möglich auf einen Webserver auf dem Terminal zuzugreifen. Wenn dies erfordert wird, so muss die erste Regel entfernt werden.

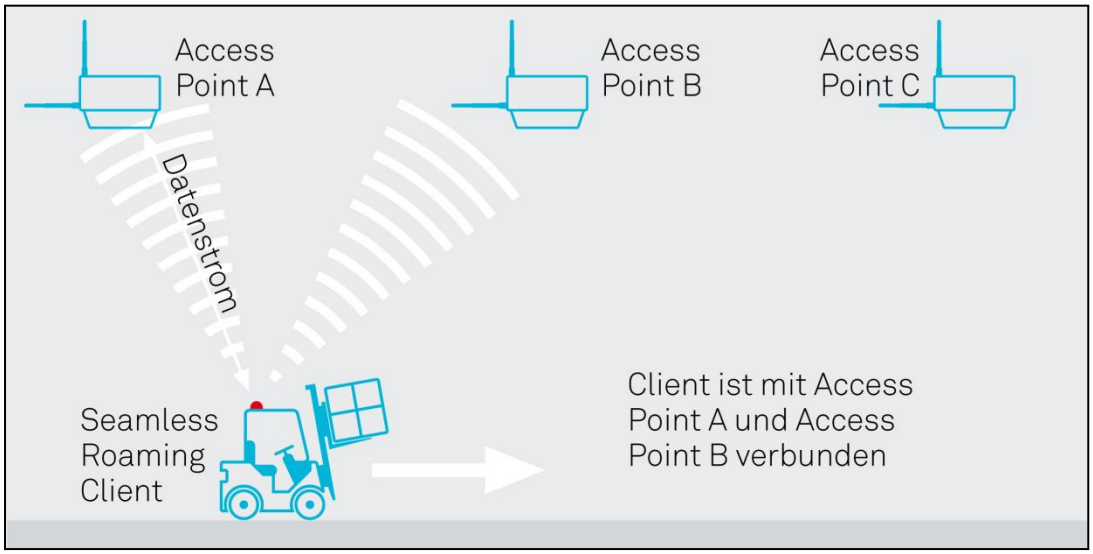
12.7 SEAMLESS ROAMING

ALLGEMEIN

Ziel des Seamless Roamings ist es, den Roamingvorgang ohne Paketverluste zu bewerkstelligen. Hierzu sind ausschließlich Dual WLAN Geräte in der Lage, da diese mit zwei WLAN Schnittstellen ausgestattet sind. Diese beiden Schnittstellen werden identisch konfiguriert. Während eine Schnittstelle die Datenkommunikation übernimmt, wie sie vom normalen WLAN her bekannt ist, versucht die zweite Schnittstelle eine Verbindung mit höherer Signalstärke zu finden. Mit Hilfe dieser Funktionalität lassen sich komplexe Netzwerke mit mehreren Access-Points aufbauen, in denen sich der Client relativ zügig frei bewegen kann, ohne dass Paketverluste durch das Roaming auftreten.

Die Konfiguration eines Seamless Roaming Clients unterscheidet sich nur gering von der Konfiguration eines normalen WLAN Clients. Die Konfiguration der Access-Points unterscheidet sich nicht von der Konfiguration anderer Access-Points und wird daher hier nicht erläutert.

Hinweis:
Der RAC112 benötigt, um seine Seamless Roaming Funktionalität anzuwenden, Geräte der RAP Produktserie ab Version 3.1.


Access Point A
Access Point B
Access Point C
Datenstrom
Seamless Roaming Client
Client ist mit Access Point A und Access Point B verbunden

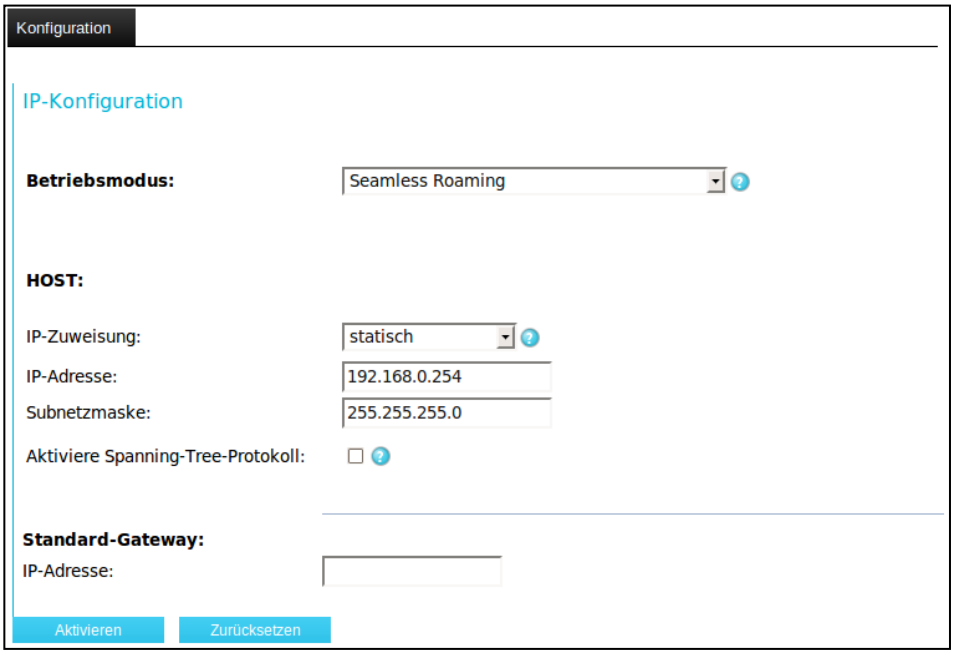
KONFIGURATION DES SEAMLESS ROAMING MODUS

Basiskonfiguration

Um das Gerät in den Seamless Roaming Modus zu setzen muss man den Betriebsmodus unter „**Konfiguration → IP-Konfiguration**“ in **Seamless Roaming** ändern.

Hinweis:
Sobald das Gerät im Seamless Roaming Modus betrieben wird, sind die Konfigurationsseiten für die zweite WLAN-Schnittstelle inaktiv!

Hinweis:
Für beide WLAN-Schnittstellen wird das Nachbar-Roaming deaktiviert, dies wird auch nach dem Deaktivieren des Seamless Roaming Modus beibehalten!



KONFIGURATION DER WLAN SCHNITTSTELLE

Die weitere Konfiguration der WLAN-Schnittstelle kann wie gewohnt unter

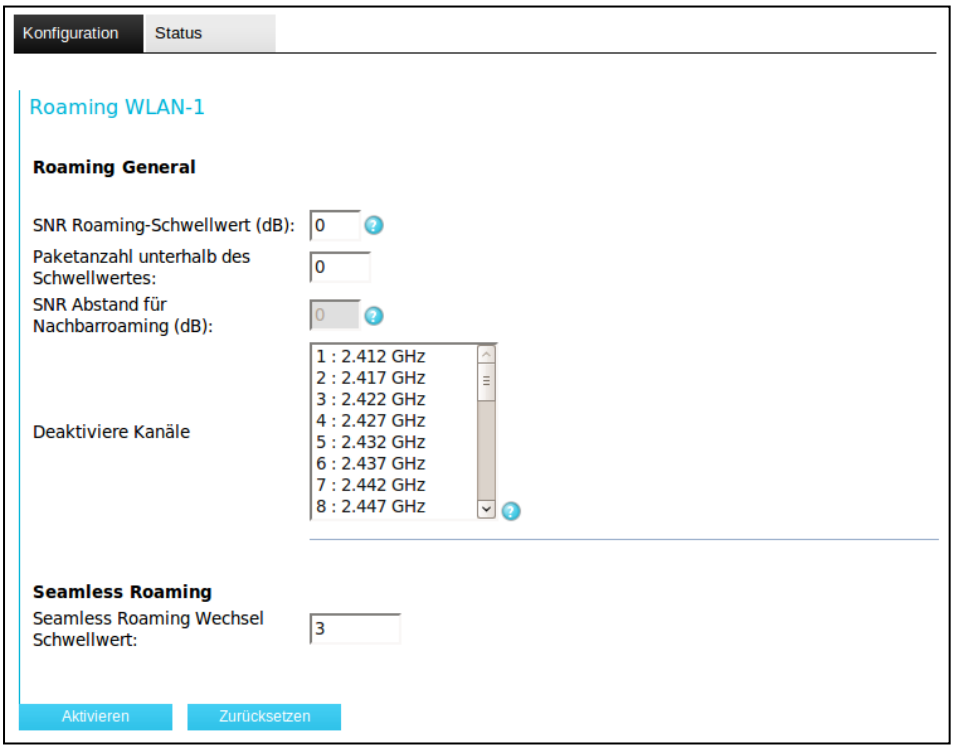
- **Konfiguration → WLAN-1 Parameter**
- **Konfiguration → WLAN-1 Sicherheit**
- **Konfiguration → Adv. WLAN** /

vorgenommen werden.

Dabei kann nur die WLAN-1 Schnittstelle konfiguriert werden, die Einstellungen werden automatisch auf die zweite Schnittstelle angewandt.

Hinweis:

Die Antenneneinstellungen können weiterhin für beide WLAN-Schnittstellen auf den jeweiligen Seiten vorgenommen werden.



KONFIGURATION DES SEAMLESS ROAMING VERHALTENS

Unter „**Konfiguration → Adv. WLAN → Roaming WLAN-1**“ kann der Wechsel Schwellenwert für das Seamless Roaming angegeben werden. Dieser Schwellenwert gibt an, ab wann eine Verbindungsqualität der einen WLAN-Schnittstelle der Verbindungsqualität der anderen Schnittstelle vorzuziehen ist.

Beispiel:

Beide Schnittstellen seien konfiguriert und momentan bei einem Access-Point eingebucht.

Verbindungsqualität WLAN-1: 23 dB
Verbindungsqualität WLAN-2: 38 dB

Damit das Gerät nun die zweite Schnittstelle als „Bessere“ ansieht muss der Seamless Roaming Wechsel Schwellenwert kleiner als 15dB sein.

DEAKTIVIEREN DES SEAMLESS ROAMING MODUS

Der Betriebsmodus kann unter „**Konfiguration → IP-Konfiguration**“ wieder verändert werden (Standardmäßig Transparent-Bridge).

Hinweis:

Nach dieser Umstellung bleiben die Einstellungen der WLAN-1 Schnittstelle erhalten. Die zweite WLAN Schnittstelle erhält wieder die Einstellungen, die vor der Aktivierung des Seamless Roaming Modus verwendet wurden!

Einfluss der erweiterten Roaming Parameter

Unter „**Konfiguration → Adv. WLAN → Roaming WLAN-1**“ können die erweiterten Roaming Parameter eingestellt werden.

Das Nachbar Roaming ist im Seamless Roaming Modus deaktiviert. Die beiden anderen Roaming Parameter können angewandt werden.

Über die Eingeschränkte Kanalliste kann der Scanvorgang beider Schnittstellen verkürzt werden. Die beiden Felder „**SNR Roaming Schwellenwert**“ und „**Paketanzahl unterhalb des Schwellenwerts**“ können zum Erkennen schlechter werdender Verbindungen verwendet werden. Hierbei ist aber zu beachten, dass sich die Parameter nur auf die passive Schnittstellen beziehen, damit die aktive Datenverbindung nicht negativ beeinflusst wird.

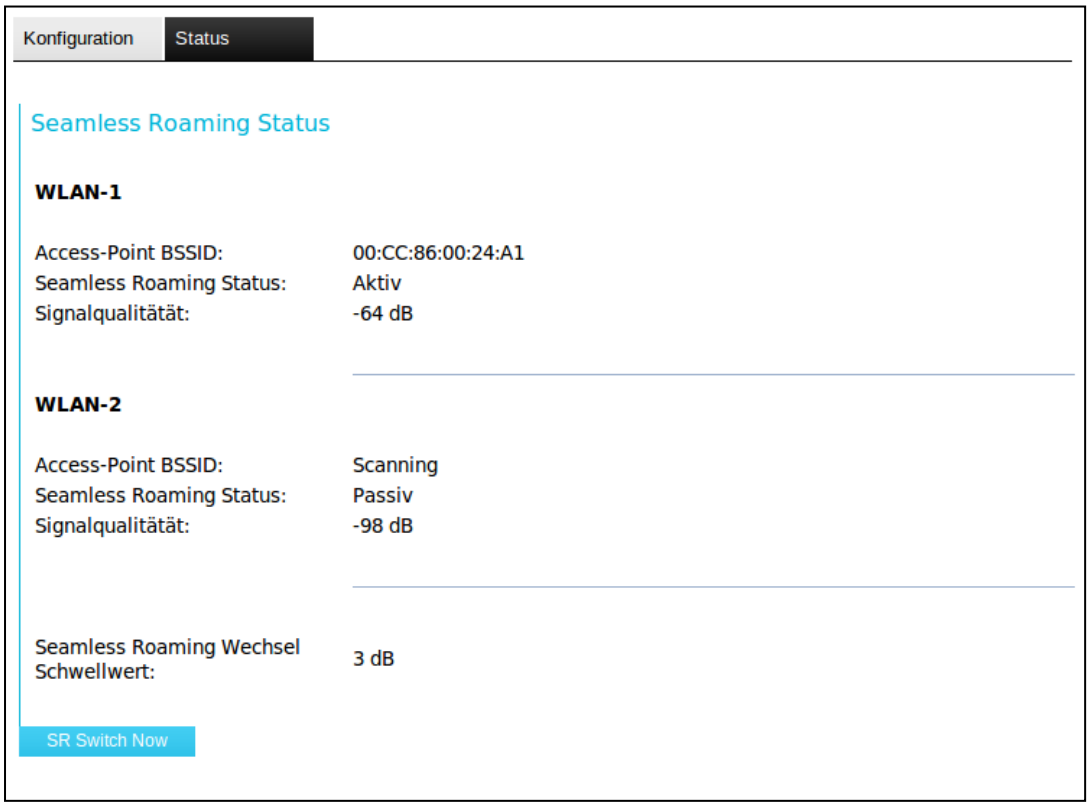
Statusausgaben im Seamless Roaming

Neben den bekannten Statusnachrichten kommen in der Ereignisanzeige noch weitere Seamless Roaming spezifische hinzu, wenn eine „bessere“ Verbindung gefunden wird so taucht die Meldung „**Switching from WLAN-1 to WLAN-2**“ auf. Des Weiteren wird die Schnittstelle, die nach besseren Verbindungen sucht, permanent Statusnachrichten und ggf. auch WPA Nachrichten erzeugen, **dies ist kein Fehlverhalten**.

Eventlog

```
Mar  1 19:55:24 RAC212x-AX00900129 kernel: WLAN-2 send disassociate to 00:cc:86:00:24:a0 (reason code 8)
Mar  1 19:55:24 RAC212x-AX00900129 wlan: SR: FSM Switching from WLAN-2(00:cc:86:00:24:a1) to WLAN-1(00:cc:86:00:24:a1).
Mar  1 19:55:23 RAC212x-AX00900129 wpa_supplicant: WLAN-1 WPA: Key negotiation completed with 00:cc:86:00:24:a1 [PTK=CCMP GTK=CCMP]
Mar  1 19:55:23 RAC212x-AX00900129 kernel: WLAN-1: associated to access point: 00:cc:86:00:24:a1 SNR 65dB
Mar  1 19:55:17 RAC212x-AX00900129 kernel: WLAN-1 send disassociate to 00:cc:86:00:24:a1 (reason code 8)
Mar  1 19:55:12 RAC212x-AX00900129 wpa_supplicant: WLAN-1 WPA: Key negotiation completed with 00:cc:86:00:24:a1 [PTK=CCMP GTK=CCMP]
Mar  1 19:55:12 RAC212x-AX00900129 kernel: WLAN-1: associated to access point: 00:cc:86:00:24:a1 SNR 63dB
Mar  1 19:55:05 RAC212x-AX00900129 kernel: WLAN-1 send disassociate to 00:cc:86:00:24:a1 (reason code 8)
Mar  1 19:55:00 RAC212x-AX00900129 wpa_supplicant: WLAN-1 WPA: Key negotiation completed with 00:cc:86:00:24:a1 [PTK=CCMP GTK=CCMP]
Mar  1 19:55:00 RAC212x-AX00900129 kernel: bond0: received packet with  own address as source address
Mar  1 19:55:00 RAC212x-AX00900129 kernel: WLAN-1: associated to access point: 00:cc:86:00:24:a1 SNR 63dB
Mar  1 19:54:53 RAC212x-AX00900129 kernel: WLAN-1 send disassociate to 00:cc:86:00:24:a1 (reason code 8)
Mar  1 19:54:53 RAC212x-AX00900129 wlan: SR: FSM Switching from WLAN-1(00:cc:86:00:24:a0) to WLAN-2(00:cc:86:00:24:a0).
```

Auf der WLAN Diagnose Seite wird angezeigt, ob sich die Schnittstelle gerade Daten versendet (Seamless Roaming Status Aktiv) oder ob die Schnittstelle nach besseren Verbindungen sucht (Passiv). Die Scan Ergebnisse der beiden Schnittstellen können sich unterscheiden, da verhindert werden muss, dass nicht beide Schnittstellen den gleichen Access-Point auswählen. Deshalb ist es möglich, dass die passive Schnittstelle nicht den Access-Point der Aktiven sieht und vice versa.


Konfiguration
Status
Seamless Roaming Status
WLAN-1
Access-Point BSSID:
00:CC:86:00:24:A1
Seamless Roaming Status:
Aktiv
Signalqualität:
-64 dB
WLAN-2
Access-Point BSSID:
Scanning
Seamless Roaming Status:
Passiv
Signalqualität:
-98 dB
Seamless Roaming Wechsel Schwellwert:
3 dB
SR Switch Now

12.8 Extended Backround Scanning

Allgemein

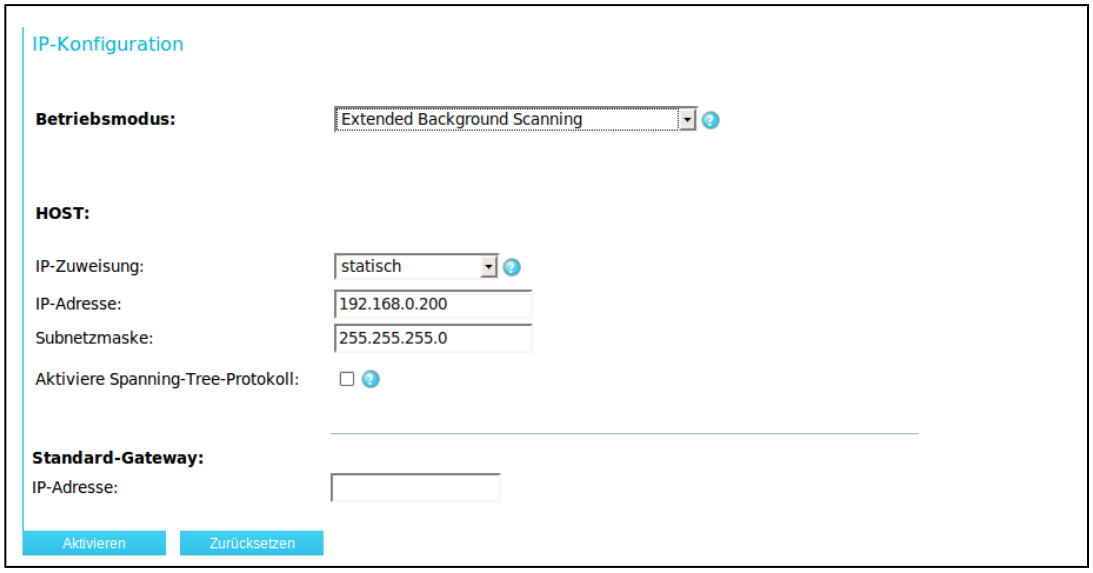
Ziel des Extended Background Scanning ist es, den Roamingvorgang ohne Zeitverluste beim Scanning zu realisieren. Hierzu werden 2 WLAN-Schnittstellen benötigt, deshalb ist ausschließlich der RAC112 dazu in der Lage, da er als einziger Client mit zwei WLAN Schnittstellen ausgestattet ist. Diese beiden Schnittstellen werden identisch konfiguriert. Während eine Schnittstelle die Datenkommunikation übernimmt, wie sie vom normalen WLAN her bekannt ist, scannt die zweite Schnittstelle permanent und liefert die neue Informationen an die erste Schnittstelle. Mit Hilfe dieser Informationen und dem Schwellenwert für das Nachbar Roaming kann die erste Schnittstelle neue Access-Points bewerten und gegebenenfalls zu diesen Roamen. Dabei fällt die Zeitdauer für das Scanning weg, da der Kanal und die Adresse des besseren Access-Points bereits bekannt sind.

Die Konfiguration eines Extended Background Scanning Clients unterscheidet sich nur gering von der Konfiguration eines normalen WLAN Clients. Die Konfiguration der Access-Points unterscheidet sich nicht von der Konfiguration anderer Access-Points und wird daher hier nicht erläutert.

Konfiguration

Aktivieren des Extended Background Scanning Modus

Um den RAC112 in den Extended Background Scanning Modus zu setzen muss man den Betriebsmodus unter „**Konfiguration → IP-Konfiguration**“ in Extended Background Scanning ändern.



Hinweis:

Sobald der RAC112 im Extended Background Scanning betrieben wird, sind die Konfigurationsseiten für die zweite WLAN-Schnittstelle inaktiv!

Hinweis:
Für beide WLAN-Schnittstellen wird das Nachbar-Roaming aktiviert, dies wird auch nach dem Deaktivieren des im Extended Background Scanning Modus beibehalten!

KONFIGURATION DER WLAN-SCHNITTSTELLE(N)

Die weitere Konfiguration der WLAN-Schnittstelle kann wie gewohnt unter

Konfiguration → WLAN-1 Parameter
Konfiguration → WLAN-1 Sicherheit
Konfiguration → Adv. WLAN /

vorgenommen werden.

Dabei kann nur die WLAN-1 Schnittstelle konfiguriert werden, die Einstellungen werden automatisch auf die zweite Schnittstelle angewandt.

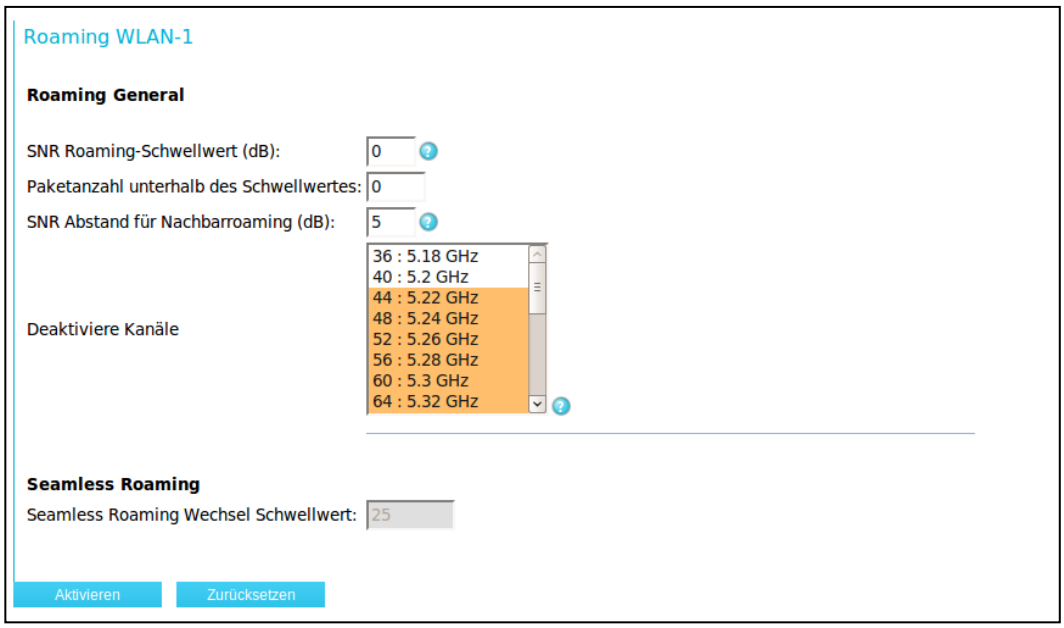
Hinweis:
Die Antenneneinstellungen können für beide WLAN-Schnittstellen auf den jeweiligen Seiten vorgenommen werden.

ERWEITERTE KONFIGURATION DES EXTENDED BACKGROUND SCANNINGS

Unter „**Konfiguration → Adv. WLAN → Roaming WLAN-1**“ kann der Wechsel Schwellenwert für das Extended Background Scanning angegeben werden. Dieser Schwellenwert gibt an, ab wann eine Verbindungsqualität der einen WLAN-Schnittstelle der Verbindungsqualität der anderen Schnittstelle vorzuziehen ist. Dabei wird der gleiche Schwellenwert wie für die Nachbar Roaming Funktionalität verwendet.

Beispiel:
Beide Schnittstellen seien konfiguriert und momentan bei einem Access-Point eingebucht.

Verbindungsqualität WLAN-1: 23 dB
Verbindungsqualität WLAN-2: 38 dB



Damit der RAC112 nun die zweite Schnittstelle als „Bessere“ ansieht muss der SNR Abstand kleiner als 15 sein. Aber er darf nicht deaktiviert (auf 0 gesetzt) werden. Hier im Bild 5dB.

Einfluss der erweiterten Roaming Parameter

Unter „**Konfiguration → Adv. WLAN → Roaming WLAN-1**“ können die erweiterten Roaming Parameter eingestellt werden.

Das Nachbar Roaming muss bei einem RAC112 im Extended Background Scanning Modus aktiviert sein. Die beiden anderen Roaming Parameter können aber zur weiteren Verbesserung des Roamings angewandt werden. Über die Eingeschränkte Kanalliste kann der Scanvorgang beider Schnittstellen verkürzt werden. Die beiden Felder „SNR Roaming Schwellenwert“ und „Paketanzahl unterhalb des Schwellenwerts“ können zum Erkennen schlechter werdender Verbindungen verwendet werden. Hierbei ist aber zu beachten, dass sich die Parameter auf beide Schnittstellen beziehen und wenn diese falsch gewählt werden, kann auch die aktive Datenverbindung negativ beeinflusst werden..

Statusausgaben im Extended Background Scanning Modus

Hat die aktive Schnittstelle von der scannenden Schnittstelle einen besseren Access-Point erhalten, so tauch im Eventlog die Nachricht:

„WLAN-1: found better access point: 00:11:22:33:44:55 on channel 10“

Deaktivieren des Extended Background Scanning Modus

Der Betriebsmodus kann unter „Konfiguration → IP-Konfiguration“ wieder verändert werden (Standardmäßig Transparent-Bridge).

Hinweis:

Nach dieser Umstellungen bleiben die Einstellungen der WLAN-1 Schnittstelle erhalten. Die zweite WLAN Schnittstelle erhält wieder die Einstellungen, die vor der Aktivierung des Extended Background Scanning verwendet wurden!

12.9 ERWEITERTE ROAMING PARAMETER

ALLGEMEIN

Roaming wird immer dann benötigt, wenn sich ein Client auf einer großen Fläche bewegt, die nicht nur von einem Access-Point abgedeckt werden kann. Im Vergleich zu Richtfunk oder Point to Point Verbindungen, die meist eine fixe Kanalwahl haben, müssen bei Roaming Setups die Clients in der Lage sein die verschiedenen Access-Points auf unterschiedlichen Kanälen zu finden.

Beim Roaming sind prinzipiell zwei Kenngrößen von Bedeutung:

- **Wann**

  und

- **Wohin**

Zum Einen muss der Client wissen oder sich entscheiden zu welchem Zeitpunkt er eine bestehende Verbindung aufgibt und nach einer Besseren sucht. Zum Zweiten kommt zusätzlich die Frage auf, wo sich denn ein besserer Access-Point befindet.

Für die erste Kenngröße werden folgende Werte betrachtet und unter „Roaming Schwellenwert“ erläutert:

Verbindungsqualität

Zeitdauer

Neben diesem „aktiven“ Roaming kann der Client auch permanent Informationen auswerten, die sowieso schon in der Luft von anderen Netzwerken enthalten sind. Dies wird im Abschnitt „Nachbar Roaming“ behandelt.

Die zweite Kenngröße „Wohin“ bestimmt am stärksten die Zeitdauer des Verbindungsausfalls. Muss ein Client erst wieder alle Kanäle abscannen vergeht eine recht lange Zeit. Deshalb bieten die Clients die Möglichkeit die Kanalliste einzuschränken, siehe „Eingeschränkte Kanalliste“

Die Konfiguration der WLAN-Schnittstelle kann wie gewohnt unter

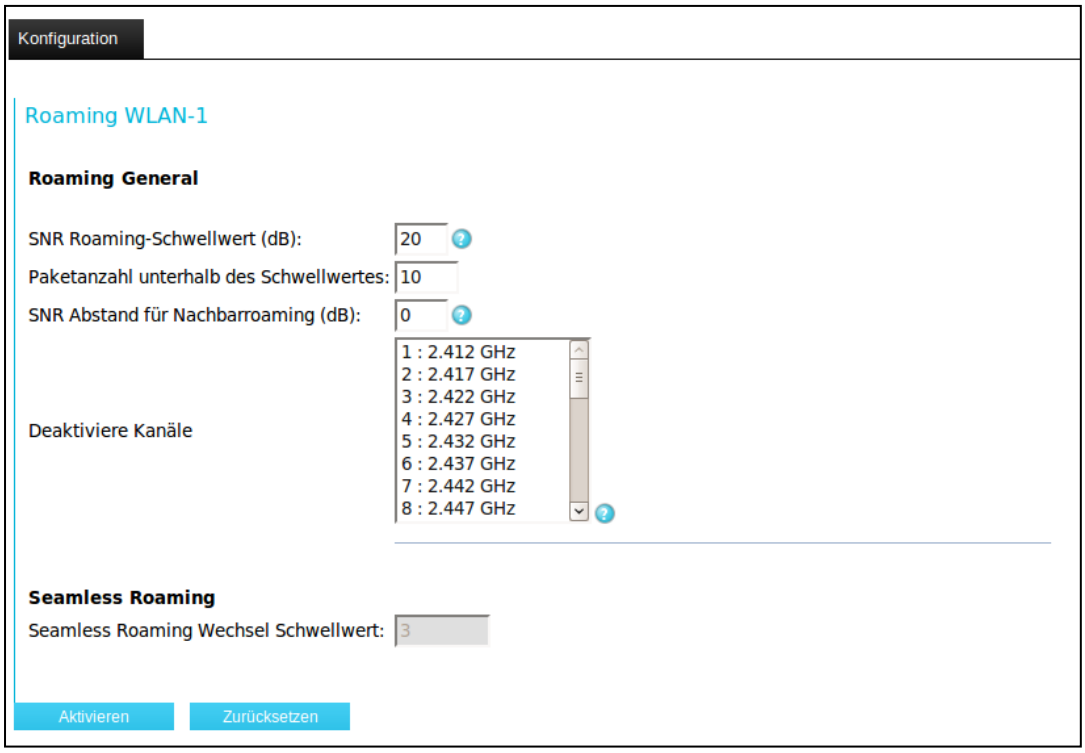
- **Konfiguration → WLAN-1 Parameter**
- **Konfiguration → WLAN-1 Sicherheit**
- **Konfiguration → Adv. WLAN /**

vorgenommen werden. Danach können die Roaming Parameter, wie in den nachfolgenden Abschnitten erklärt, verfeinert werden.

KONFIGURATION

Roaming Schwellenwert

Um einen Client schon vor dem Verlieren der Verbindung zu einem Access-Point roamen zu lassen, können die Parameter „**SNR-Roaming Schwellenwert**“ und „**Paketanzahl unterhalb des Schwellenwerts**“ angepasst werden.

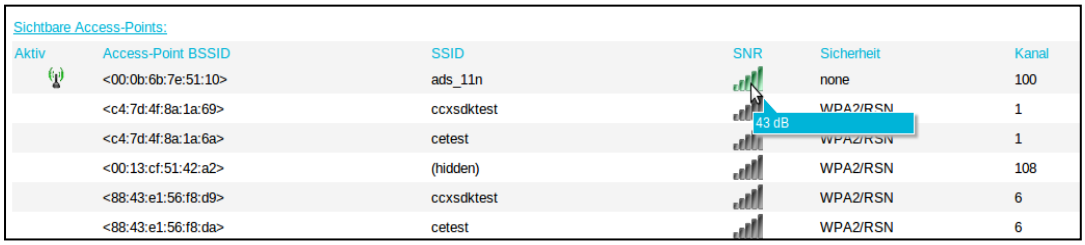


Der Schwellenwert gibt dabei die untere Grenze an, ab welcher eine Verbindung als „schlecht“ angesehen wird. Mit Hilfe der Paketanzahl kann angegeben werden ab wie vielen „schlechten“, also unterhalb des Schwellenwerts, Paketen geroamt werden soll.

Beispielhafter Ablauf einer Konfiguration

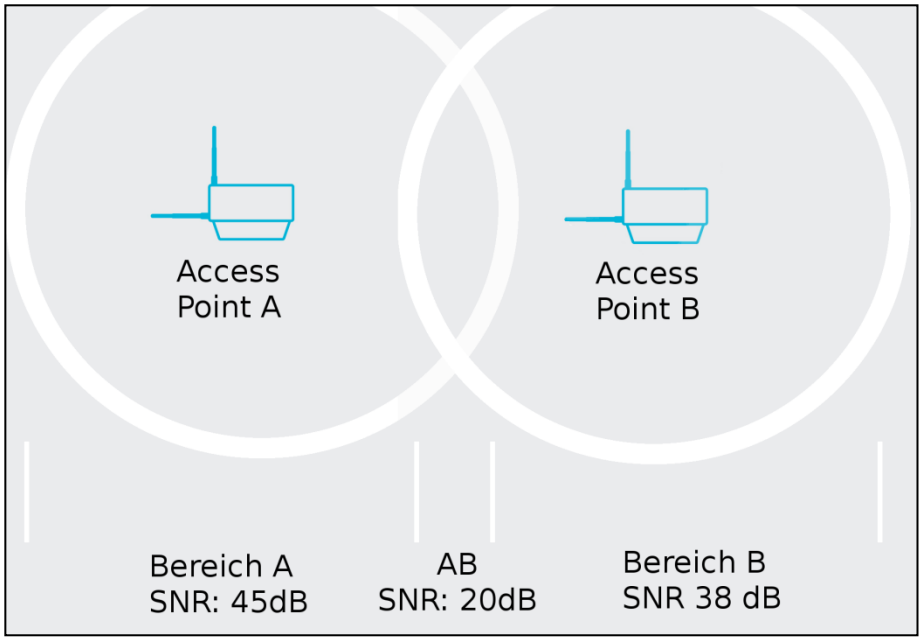
Messen der Signalstärken:

Nachdem die Access-Points fest installiert wurden, können die momentanen SNR(Signal Noise Ratio) Werte im Webinterface unter „**Diagnose → WLAN1 Parameter**“ eingesehen werden. Nun sollten auf dem gesamten Gelände die Singalstärken zu den Access-Points gemessen werden. Zumindest sollten die Punkte direkt an den Access-Points und zwischen einem oder mehreren Access-Points erfasst werden.



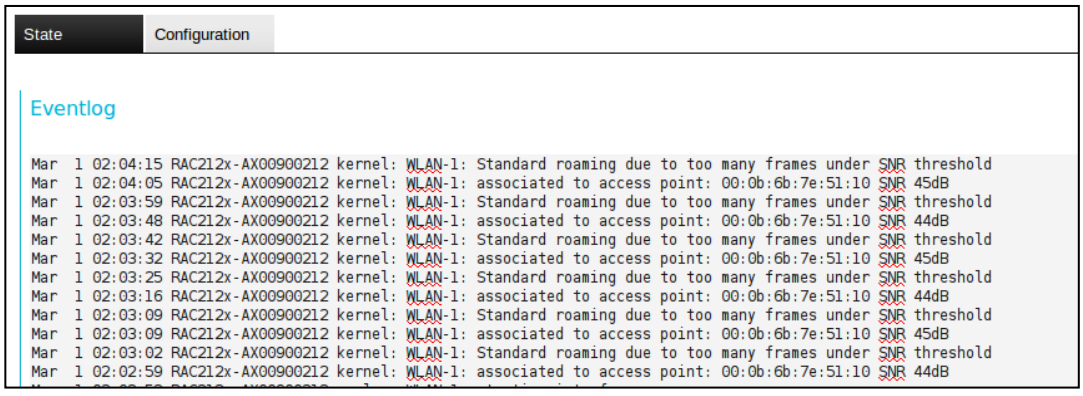
Bestimmen des Schwellenwerts:

Der Schwellenwert sollte so gewählt werden, dass er ein wenig Unterhalb des geringsten Schwellenwerts liegt, der zwischen allen Access-Points gemessen wurde. Er darf aber niemals über den Signalstärken liegen, der direkt an den Access-Points gemessen wurde. In der Abbildung unten sind die Signalstärken in den Bereichen A und B recht hoch (45 und 38 dB). Im überlappenden Bereich AB ergibt sich eine Signalstärke von 20dB, deshalb sollte der Schwellenwert bei 20dB gewählt werden, damit der Client bei kleineren Signalstärken roamt.



Vornehmen der Einstellungen:

Es empfiehlt sich, die Paketanzahl fix zu lassen (z.B.: 15) und zuerst denn Schwellenwert einzustellen (im Bsp.: 15), danach kann bei zu langem Verweilen die Paketanzahl verringert oder bei zu häufigem Roamen die Paketanzahl erhöht werden. Schlagen die Roamingtrigger an, so tauchen im Eventlog des Clients folgende Meldungen auf:


State
Configuration
Eventlog
Mar 1 02:04:15 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:04:05 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 45dB
Mar 1 02:03:59 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:03:48 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 44dB
Mar 1 02:03:42 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:03:32 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 45dB
Mar 1 02:03:25 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:03:16 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 44dB
Mar 1 02:03:09 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:03:09 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 45dB
Mar 1 02:03:02 RAC212x-AX00900212 kernel: WLAN-1: Standard roaming due to too many frames under SNR threshold
Mar 1 02:02:59 RAC212x-AX00900212 kernel: WLAN-1: associated to access point: 00:0b:6b:7e:51:10 SNR 44dB

Fehlerursachen:

Zu viele Roaming Meldungen innerhalb kurzer Zeit. im Eventlog des Clients deuten auf einen zu hohen Schwellenwert hin oder die Paketanzahl ist zu niedrig gewählt

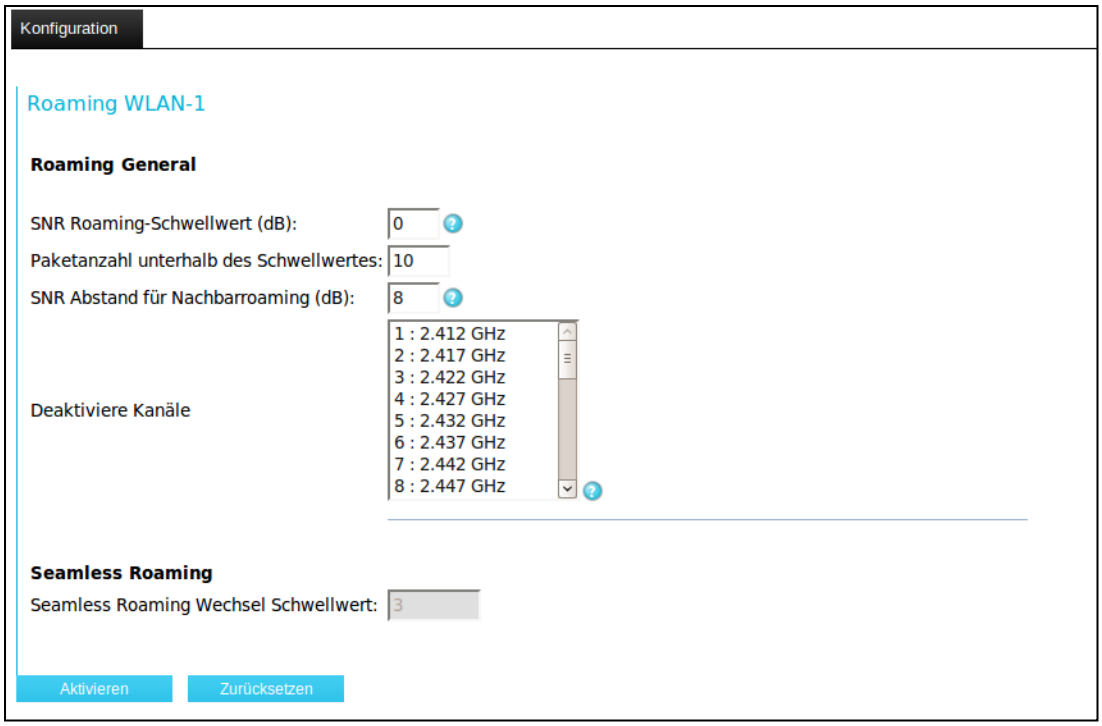
Zu langes Verweilen bei einem Access-Point dagegen auf einen zu niedrigen Schwellenwert oder zu hohe Paketanzahl.

Hinweis:
Ein Schwellenwert von „0“ deaktiviert diese Funktion!

Hinweis:
Erfahrungswerte haben gezeigt, dass für die „Paketanzahl unterhalb des Schwellenwertes“ Werte von 10-25 Pakete und für den „Schwellenwert“ Werte im Bereich von 15-25 dB gute Resultate erzielen!

Nachbar Roaming:

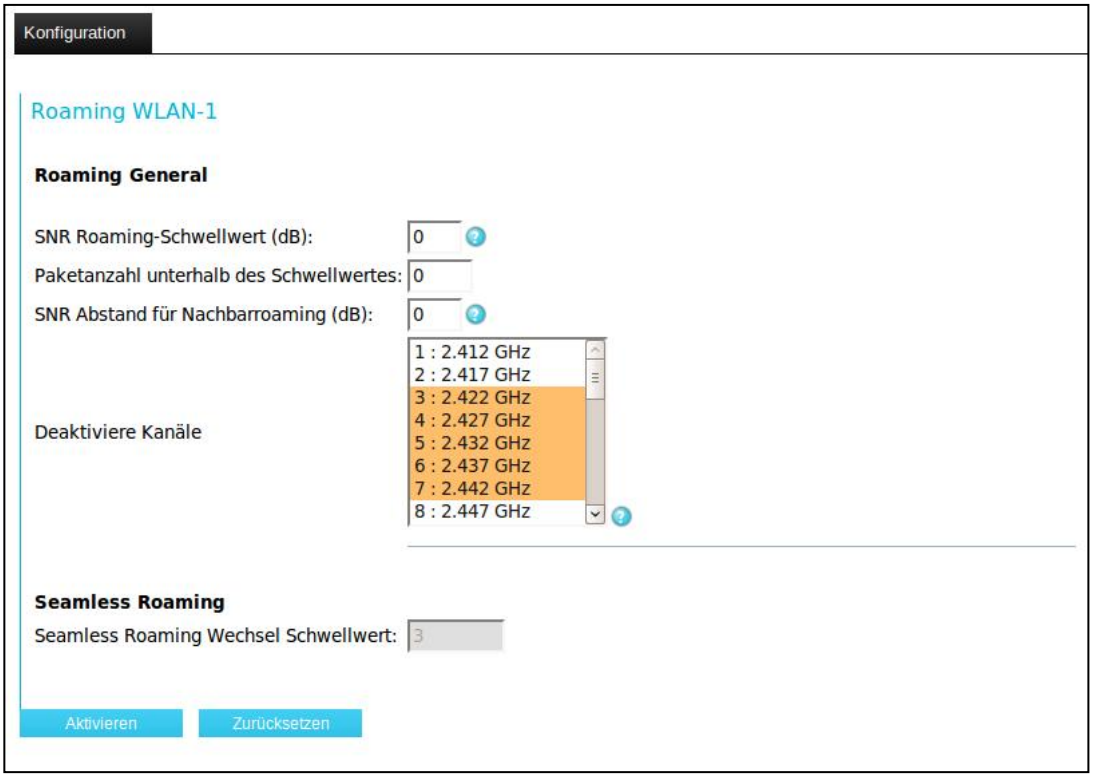
Unter „**Konfiguration → Adv. WLAN → Roaming WLAN**“ kann der „**SNR Abstand**“ für das Nachbar Roaming angegeben werden. Dieser Schwellenwert gibt an, ab wann eine Verbindungsqualität eines Access-Points auf einem direkt benachbarten Kanal der Verbindungsqualität des aktuellen Access-Points vorzuziehen ist.



Hinweis:
Ein SNR Abstand von „0“ deaktiviert das Nachbar Roaming!

EINGESCHRÄNKTE KANALLISTE

Unter „**Konfiguration → Adv. WLAN → Roaming WLAN**“ können die Kanäle, die ein Client auf Access-Points überprüft, eingeschränkt werden. Hierzu können mit der linken Maustaste und gleichzeitigem drücken der Strg- oder Shift Tasten eine Auswahl getroffen werden. Die selektierten Kanäle werden dann nicht vom Client verwendet, sie sind deaktiviert.



Hinweis:
Werden alle Kanäle ausgewählt, so wird der Client keinen Access-Point finden.

12.1 REMOTE CAPTURE

ALLGEMEIN

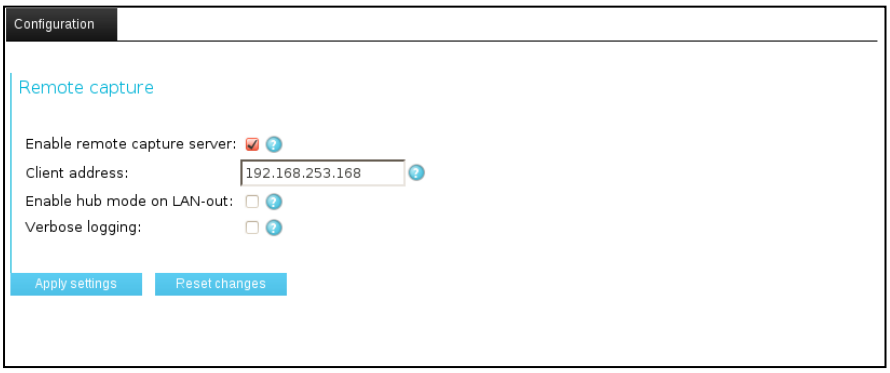
Mit Remote-Capture kann der Verkehr einer beliebigen, aktiven Geräte-Schnittstelle über Netzwerk von einem Windows-Rechner mit Wireshark (**http://www.wireshark.org**). aufgezeichnet und analysiert werden.

Hinweis:

Dieses Feature ist nur zum Debuggen gedacht. Weil eine Authentifizierung nicht möglich ist, sollte der Capture-Server nur bei Bedarf kurzzeitig zu Diagnosezwecken aktiviert werden, um das Sicherheitsrisiko zu minimieren.

KONFIGURATION

Der Remote-Capture-Service kann unter Diagnose/Remote-Capture aktiviert werden und lauscht dann auf dem Standardport 2002 auf eingehende Verbindungen. Weil keine Authentifizierung möglich ist, muss die IP-Adresse des Rechners, der die Aufnahme machen soll, explizit angegeben werden (z.B. 192.168.253.168), um das Sicherheitsrisiko zu minimieren:



Als weitere Sicherheitsmaßnahme darf nur eine Verbindung auf einmal bestehen, d.h. der genannte Rechner kann keine zwei Aufnahmen gleichzeitig durchführen.

LAN-out funktioniert normalerweise als Switch. Das heißt, wenn sich zwei Geräte (z.B. an Port 1 und Port 2) unterhalten, werden die Pakete hardwaremäßig innerhalb des Switches weitergeleitet, erreichen also nicht das Geräte-System und können damit auch nicht aufgezeichnet werden. Um sämtlichen Verkehr zwischen den Ports bei Bedarf sichtbar zu machen, kann die Option Aktiviere Hub-Modus für LAN-out verwendet werden. Im Hub-Modus werden sämtliche Pakete an alle Ports und auch an das Geräte-System weitergereicht.

Normalerweise werden nur Zugriffsverletzungen mitgeloggt (Verbindungsaufbau von falscher IP-Adresse oder zweiter Verbindungsversuch). Mit Detaillierte Meldungen werden auch Informationen über die Verbindung (Kontroll/Datenkanal) und abgehörte Schnittstellen vermerkt.

Hinweis:

Damit der Service nicht aus Versehen unwissentlich läuft, wird stündlich eine Warnung im Eventlog ausgegeben.

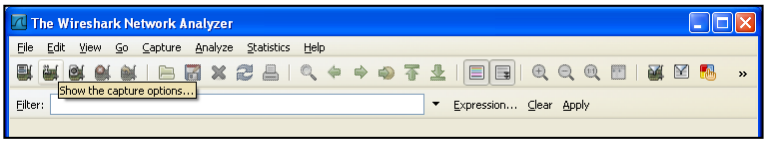
Um eine sinnvolle Aufzeichnung zu gewährleisten, wird die Remote-Capture-Verbindung zwischen dem Gerät und dem aufnehmenden Rechner grundsätzlich gefiltert.

Der Hub-Modus braucht ungefähr 10 Sekunden bis er aktiv ist. Wird also ein Remote-Capture zu schnell gestartet, sieht man unter Umständen die ersten Pakete nicht in der Aufnahme.

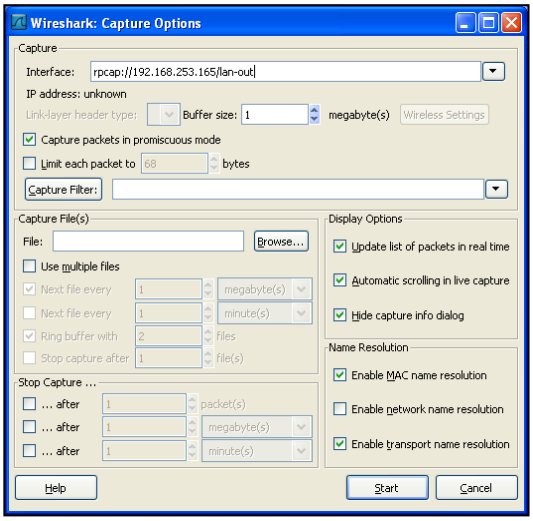
KONFIGURATION WIRESHARK UNTER WINDOWS XP

Es muss mindestens Wireshark in der Version 1.0.6 und WinPcap in der Version 4.0.2 verwendet werden. In früheren Versionen war es nicht möglich, eine Aufnahme zu stoppen oder erneut zu starten.

Remote-Schnittstellen müssen explizit unter Show the capture options (zweites Icon in der Hauptwerkzeugleiste) oder im Menü unter Capture/Options angegeben werden:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Show the capture options...
Filter:
Expression... Clear Apply

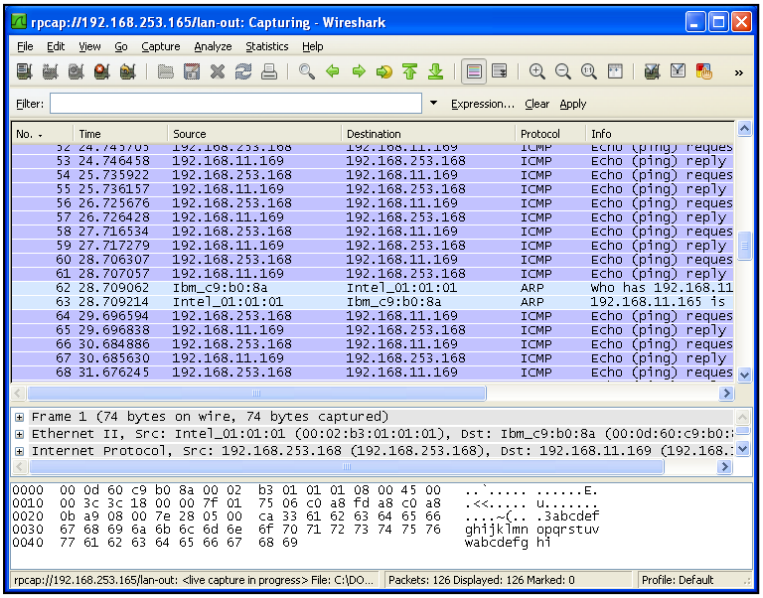
Um zum Beispiel den Verkehr auf LAN-out des Gerätes mit der IP-Adresse 192.168.253.165 mitzuschneiden, lautet die Remote-Capture-URL rpcap://192.168.253.165/LAN-out:

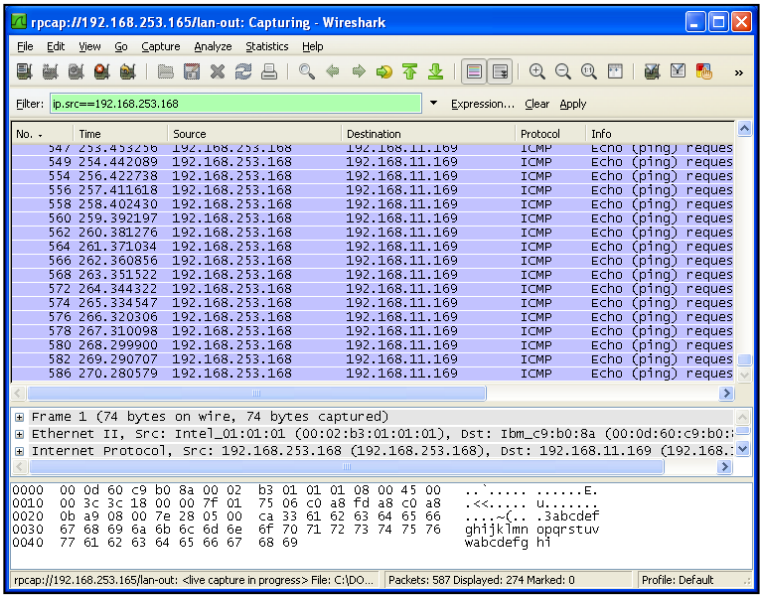


Der Prefix rpcap:// ist immer anzugeben und kennzeichnet die Aufnahme per Netzwerk. Die Schnittstellen des Gerätes können ohne Beachtung der Groß- und Kleinschreibung entsprechend der im Webinterface verwendeten Namen angegeben werden. Ausnahmen sind die IPsec-Schnittstellen – dort muss das Leerzeichen vor dem (IPsec) weggelassen werden – und die PPPoE-Schnittstelle, die über dsl oder pppoe angesprochen werden kann. Konkret sind folgende Bezeichnungen möglich:

Schnittstelle	Bemerkung
DSL PPPoE	PPPoE-Uplink (unabhängig von der zugrunde liegenden Schnittstelle, über die die Verbindung zustande gekommen ist)
LAN-in	Existiert immer
LAN-out	Existiert immer
LAN-out-x	Die einzelnen Ports (x ist mit 1,2,3 oder 4 zu ersetzen) existieren nur im erweiterten IP-Routermodus. LAN-out ist dann der interne Endpunkt für Layer 2 OpenVPN-Verbindungen.
SERVICE	Existiert, falls eine Modemverbindung besteht
L2-VPNx	Die einzelnen OpenVPN-Schnittstellen (x ist mit 1 bis 10 zu ersetzen) existieren bei Master-Verbindungen immer und bei Clientverbindungen nur, wenn sich der Client tatsächlich verbunden hat.
LAN-in(IPsec) LAN(IPsec) LAN-out-1(IPsec) LAN-out-2(IPsec) LAN-out-3(IPsec) LAN-out-4(IPsec) SERVICE(IPsec)	Entsprechend der IPsec-Konfiguration gibt es für den Tunnelendpunkt eine bestimmte IPsec-Schnittstelle (z.B. LAN-in(IPsec)), auf der der Verkehr unverschlüsselt sichtbar ist. Auf der zugrundeliegenden Schnittstelle (z.B. LAN-in) sind nur die verschlüsselten Pakete zu sehen. LAN(IPsec) gehört zum Tunnelendpunkt für LAN-out.

Wenn die Verbindung erfolgreich zustande gekommen ist, können die Pakete unter Wireshark ganz normal betrachtet und gefiltert werden:





Hinweis:

Sollte die Windows-Firewall aktiviert sein, genügt es nicht, den Port 2002 frei zu schalten, weil ähnlich wie bei FTP eine separate Datenverbindung mit beliebigen Portnummern verwendet wird. Das ads-tec Gerät, auf der der Remote-Capture-Server läuft, benötigt keine besonderen Filtereinstellungen.

WIRESHARK-FEHLERMELDUNGEN

Falls der Verbindungsaufbau fehlschlägt, zeigt Wireshark ein Fenster mit der Meldung The capture session could not be initiated und einer genauen Begründung in Klammern. Im Folgenden sind die häufigsten Gründe erklärt.

ioctl: No such device

Die angegebene Schnittstelle existiert nicht. Entweder ist die Schreibweise falsch (siehe obige Tabelle), das Gerät anders konfiguriert oder die Schnittstelle temporär nicht verfügbar (z.B. existiert die PPPoE-Schnittstelle nur bei bestehendem Uplink).

Is the server properly installed on <IPADDRESS>? connect() failed: ...

Die angegebene IP-Adresse <IPADDRESS> ist nicht erreichbar oder der Remote-Capture-Service läuft dort nicht.

The host is not in the allowed host list. Connection refused.

Die IP-Adresse des eigenen Rechners entspricht nicht der im Webinterface des Gerätes erlaubten (führt zu einem Eintrag im Eventlog des Gerätes).

Too many clients

Es besteht bereits eine Verbindung zum Remote-Capture-Server. Entweder durch eine andere Wireshark-Anwendung oder einen anderen Netzwerkteilnehmer mit fälschlicherweise identischer IP-Adresse (führt zu einem Eintrag im Eventlog des Gerätes).

13 CE-KONFORMITÄTSERKLÄRUNG

RAP1110

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1110-103-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	i.A. Elmar Bossler - Qualitätsmanager / *Quality Manager* - i.V. Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1111

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1111-102-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	Elmar Bössler - Qualitätsmanager / *Quality Manager* - Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1210

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1210-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009	
Name und Unterschrift *Name and signature*	Elmar Bossler - Qualitätsmanager / *Quality Manager* -	Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1211

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1211-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	i.A. Elmar Bossler - Qualitätsmanager / *Quality Manager* - i.V. Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1120

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **ads-tec GmbH** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany** **Tel. +49 (0)711-45894-0** **Fax +49 (0)711-45894-985**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1120-102-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	Elmar Bossler - Qualitätsmanager / *Quality Manager* - Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1121

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **ads-tec GmbH** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany** **Tel. +49 (0)711-45894-0** **Fax +49 (0)711-45894-985**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1121-102-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	i.A. Elmar Bossler - Qualitätsmanager / *Quality Manager* - i.V. Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1220

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1220-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1 [a]**
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009	
Name und Unterschrift *Name and signature*	i.A. Elmar Bossler - Qualitätsmanager / *Quality Manager* -	i.V. Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAP1221

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAP1000**
Type *Type*	**Industrial WLAN Access Point**
Modell *Model*	**DVG-RAP1221-102-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

i.A. Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1110

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1110-102-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009	
Name und Unterschrift *Name and signature*	Elmar Bossler - Qualitätsmanager / *Quality Manager* -	Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1111

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1111-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum *Place & date of issue*	Leinfelden-Echterdingen, 09/30/2009
Name und Unterschrift *Name and signature*	i.V. Elmar Bossler - Qualitätsmanager / *Quality Manager* - i.V. Thomas Mögerle - Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1120

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1120-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1 [a]**
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

i.A. Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1121

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1121-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Mögerle
Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik /
Manager Business Unit Data Systems -

RAC1220

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1220-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

i.A. Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1221

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **ads-tec GmbH** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany** **Tel. +49 (0)711-45894-0** **Fax +49 (0)711-45894-985**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1221-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1510

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **Tel. +49 (0)711-45894-0** **ads-tec GmbH** **Fax +49 (0)711-45894-985** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1510-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

i.A. Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

RAC1511

Konformitätserklärung

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Hersteller / Verantwortliche Person *The manufacturer / responsible person*	**Thomas Mögerle** **ads-tec GmbH** **Raiffeisenstr. 14** **70771 Leinfelden-Echterdingen / Germany** **Tel. +49 (0)711-45894-0** **Fax +49 (0)711-45894-985**
erklärt, dass das Produkt *declares that the product*	**RAC1000**
Type *Type*	**Industrial WLAN Access Client**
Modell *Model*	**DVG-RAC1511-101-BU**
Verwendungszweck *Intended purpose*	**Wireless Communication**

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

angewendete harmonisierte Normen *Harmonised standards applied*	Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a)) *Safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))* **EN 60950-1: 2006 Part 1**
angewendete harmonisierte Normen *Harmonised standards applied*	Schutzanforderungen in Bezug auf die EMV § 3 (1) 2, Artikel 3 (1) b)) *Protection requirements concerning EMC § 3(1)(2), (Article 3(1)(b))* **EN 301 489-1 V1.8.1; EN 301 489-17 V1.3.2**
angewendete harmonisierte Normen *Harmonised standards applied*	Maßnahmen zur effizienten Nutzung des Funkfrequenzspektrums *Measures for the efficient use of the radio frequency spectrum* **EN 300 328 V1.7.1; EN 301 893 V1.4.1** [a]
Schnittstellenspezifikation *Interface specification*	Luftschnittstelle bei Funkanlagen gemäß § 3(2) (Artikel 3(2)) *Air interface of the radio systems pursuant to § 3(2) (Article 3(2))*

[a] Mit Wirkung zum 1. Juli 2008 begründet diese Fassung der Norm die Vermutung der Konformität mit den Anforderungen von Artikel 3 Absatz 2 der Richtlinie 1999/5/EG, und zwar unter folgender zusätzlicher Bedingung: Der in Geräten, die im Frequenzband 5600-5650 MHz senden, verwirklichte Mechanismus der dynamischen Frequenzwahl (Dynamic Frequency Selection – DFS) muss in der Lage sein, auch solche Wetterradaranlagen zu erkennen, bei denen die zwischen den Impulsen liegenden Zeitspannen nicht konstant sind. Ihre Impulsfolgefrequenzen (Pulse Repetition Frequencies – PRF) werden oft auch als gestaffelt oder verschoben bezeichnet und können bis zu drei verschiedene Werte annehmen.
As of 1 July 2008 this version of the standard gives presumption of conformity with the requirements of article 3.2 of 1999/5/EC under the following additional condition: The Dynamic Frequency Selection (DFS) mechanism implemented by equipment transmitting in the frequency band 5600-5650 MHz, must also be able to detect meteorological radars employing non-constant pulse interval times. These are often referred to as staggered or interleaved PRFs (Pulse Repetition Frequencies) by which up to 3 different PRF values are used.

Ort, Datum
Place & date of issue: Leinfelden-Echterdingen, 09/30/2009

Name und Unterschrift
Name and signature

i.A. Elmar Bossler
- Qualitätsmanager / *Quality Manager* -

i.V. Thomas Mögerle
- Leiter Geschäftsbereich Datentechnik / *Manager Business Unit Data Systems* -

13.1 ZULASSUNG BRASILIEN

ZERTIFIKAT

REPÚBLICA FEDERATIVA DO BRASIL
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES.

ANATEL

Certificado de Homologação
(Intransferível)
Nº **0778-12-7815**
Validade: **Indeterminada**
Emissão: **18/04/2012**

Solicitante:
BRH REPRESENTAÇÃO COMERCIAL LTDA.
RUA JOSE DE ALENCAR 293 SALA 53 CENTRO
13013040 CAMPINAS SP

Fabricante:
ADS-TEC GMBH
RAIFFEISENSTRASSE 14
LEINFELDEN-ECHTERDINGEN

Outras Unidades Fabris:
ADS-TEC GMBH (WILSDRUFF)
DRESDNER TOR 1
WILSDRUFF - ALEMANHA

Este documento homologa, nos termos do Regulamento para Certificação e Homologação de Produtos para Telecomunicações, aprovado pela Resolução Anatel nº 242, de 30 de novembro de 2000, o Certificado de Conformidade nº 06351/12 , emitido pelo **OCD - IBRACE - Instituto Brasileiro de Certificação**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação do(s) serviço(s) ou aplicação(ões) a que se destina.

Tipo:
Transceptor de Radiação Restrita - Categoria II

Modelo(s):
RAP 1110
RAP 1111
RAP 1510
RAP 1511

Serviço/Aplicação:
Radiocomunicação de Radiação Restrita

Características técnicas básicas:

Faixa de Freqüências Tx (MHz)	Potência Máxima de Saída (W)	Designação de Emissões	Tecnologias	Tipo de Modulação
2400,0 a 2483,5	0,0508	12M4X9D	SEQÜÊNCIA DIRETA	DBPSK, DQPSK e CCK
2400,0 a 2483,5	0,0834	16M8X9D	OFDM	BPSK, QPSK, 16/64QAM
5150,0 a 5350,0	0,0598	-	OFDM	BPSK, QPSK, 16/64QAM
5470,0 a 5725,0	0,0908	-	OFDM	BPSK, QPSK, 16/64QAM
5725,0 a 5850,0	0,1274	16M9X9D	OFDM	BPSK, QPSK, 16/64QAM

- Os valores das potências nas faixas de 5150-5350 MHz e de 5470-5725 MHz estão em E.I.R.P. Ganho da antena: 7 dBi.
- Taxa Máxima de Transmissão: até 11 Mbit/s (sequência direta) e até 54 Mbit/s (OFDM 802.11g).

Observações:
- Ensaio de SAR: não aplicável.
- Na instalação do produto, devem ser observadas as condições de uso conforme estabelecido no Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos do art. 39 do Regulamento anexo à Resolução Anatel nº 242, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SGCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente Geral de Certificação e Engenharia do Espectro

CÓPIA

Imprimir Documento | Fechar | Voltar

ANATEL ETIKETTEN

RAP1110-103-BU

ANATEL
Agência Nacional de Telecomunicações
0778-12-7815
(01) 78989159611 62 1
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

RAP1111-102-BU

ANATEL
Agência Nacional de Telecomunicações
0778-12-7815
(01) 78989159611 63 8
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

RAP1510-101-BU

ANATEL
Agência Nacional de Telecomunicações
0778-12-7815
(01) 78989159611 64 5
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

RAP1511-101-BU

ANATEL
Agência Nacional de Telecomunicações
0778-12-7815
(01) 78989159611 65 2
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.